Privacy and Security by Design:

An Enterprise Architecture Approach

September 2013

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

Mark Dixon
Enterprise Architect, Information Security
Oracle Corporation

ORACLE®

Information and Privacy Commissioner
Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Privacy and Security by Design: An Enterprise Architecture Approach

TABLE OF CONTENTS

Foreword

As threat levels rise, security professionals are increasingly being called upon to develop new ways to protect the data assets of their organizations. The old way of simply building a defensive "perimeter" around a resource will no longer be sufficient. Rather, security must go on the *offensive* and address information security concerns as the default mode of operation of a business or organization, through an enterprise architecture approach.

I have always said that strong security is essential to achieving strong privacy. In fact, one of the 7 Foundational Principles of *Privacy by Design* is "End-to-End Security." This is echoed in a recent statement by my colleague Leslie Harris, President and CEO of the Center for Democracy & Technology, who has challenged organizations to rethink the privacy-invasive practices of the proposed Cyber Intelligence Sharing and Protection Act (CISPA) bill in the U.S. Rather than sharing highly sensitive information with government agencies, she noted that "It has to be the obligation of these tech companies to *build in security from the very beginning* [...]. You want to see these very innovative companies *step up and become leaders* in security solutions first."[1]

While security is an essential element of privacy, it is not enough – privacy and data protection subsume a much broader set of protections. *Privacy by Design* is meant to reflect a holistic approach to privacy, at an organizational or enterprise level.

In an earlier paper with Oracle, we discussed the convergence of paradigms between the approach to privacy I have long championed called *Privacy by Design*, and a similar approach to security called "Security by Design." The current and future challenges to security and privacy oblige us to revisit this convergence and delve deeper. As privacy and security professionals, we must come together and develop a proactive approach to security – one that is indeed "by design." To this end, I am delighted to be partnering with Mark Dixon, Enterprise Architect, Information Security, at Oracle Corporation, on this joint paper.

My hope is that our paper will mark a further step in the development of privacy *and* security – by design!

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

1 Bilton, N. (2013, May 6). "Disruptions: New Motto for Silicon Valley: First Security, Then Innovation," *The New York Times*. Retrieved from http://bits.blogs.nytimes.com/

1. Introduction

The close alignment between the disciplines of privacy and security was introduced in our January 2013 white paper, "Privacy and Security by Design: A Convergence of Paradigms,"[2] published jointly by the Information and Privacy Commissioner of Ontario, Canada, and Oracle Corporation. That paper laid the foundation for a further discussion between the disciplines of privacy and security. On the one hand, it noted:

> Information security professionals have come to realize that privacy is an integral part of security. By adopting such an approach early on, good privacy and security may be embedded directly into information systems, processes and architectures, thereby minimizing the likelihood of data breaches recurring in the future.[3]

On the other hand, the paper recognizes that the convergence between privacy and security is only the tip of the iceberg. In addition to a "convergence of paradigms," it points to a situation in which:

> [...] privacy and security – by design, will continue to evolve into an essential component of information technologies and operational practices of organizations, as well as becoming an integral part of entire systems of data governance and privacy protection.[4]

This follow-up paper seeks to build upon the work of our January 2013 paper by examining more closely the synergy that exists between privacy and security, and proposing steps to develop an Enterprise Security Architecture that supports the privacy-security synergy.

This paper has two key objectives:

- Define a set of foundational "Security by Design" principles that are modelled upon and support the 7 Foundational Principles of *Privacy by Design*.
- Illustrate an enterprise-level process for defining and governing the strategic journey of Security by Design through an enterprise architecture approach.

To achieve these objectives, this paper includes the following major sections, among a number of others:

- Foundational Principles of *Privacy by Design*
- Foundational Principles of Security by Design
- The Enterprise Security Journey
- Conclusion

2 Cavoukian, A., Chanliau, M. (2013). "Privacy and Security by Design: A Convergence of Paradigms." Retrieved from http://www.ipc.on.ca/images/Resources/pbd-convergenceofparadigms.pdf

3 *Ibid* p. 1.

4 *Ibid.*

In this discussion, it is important to recognize that, although the disciplines of privacy and security are closely related, they are not synonymous. Privacy seeks to respect and protect personally identifiable information by empowering individuals to maintain control over its collection, use and disclosure. Information security seeks to enable and protect activities and assets of both people and enterprises.

2. Foundational Principles of *Privacy by Design*

Although privacy requires that personally identifiable information about individuals be protected from unauthorized access, for which strong security measures are essential, it is important to recognize that privacy involves much *more* than ensuring secure access to data. In a word, privacy is all about control—enabling individuals to maintain personal control over their personally identifiable information with respect to its collection, use and disclosure. The meaning of this concept of privacy is perhaps best expressed as "informational self-determination," a term first used in a German constitutional ruling concerning personal information collected during Germany's 1983 census.

In an age where the complexity and interconnectivity of both networked systems and information and communications technologies (ICTs) are steadily increasing, challenges to privacy are growing exponentially. Privacy laws are struggling to keep up with the ever-shifting landscape brought about by such rapid technological change. Even with their growth and complexity, however, these challenges to privacy are far from insurmountable. Empowering individuals to maintain control over their personally identifiable information has not become merely a well-intentioned idea, with little hope of becoming a reality. Despite the increasing challenges brought about by the convergence of social, mobile and cloud computing, privacy is not only an achievable task but, as we will outline, a highly desirable one for organizations in maintaining the trust and confidence of their customers.

Achieving the desired outcome of privacy, moreover, does not require that one give up the many advantages and benefits of technology—for the majority of us, an impossible proposition. Rather than trying to live "off the grid," in order to achieve privacy in the Information Age, what is first required is a *change in thinking* within organizations and businesses that develop, implement and use networked systems and ICTs.

Rather than using the lens of zero-sum trade-offs, we must look at privacy and technology through the lens of positive-sum, mutually beneficial interactions. Like security, privacy need not diminish the functionality of technology. Rather, once properly understood and implemented, privacy works in conjunction with technology and enhances its functionality insofar as it increases end-user satisfaction, consumer confidence, trust and use. Technology is not hindered by privacy, but rather, made far better by it.

The key to this mutually beneficial interaction between privacy and technology is one of timing. In order to have a positive-sum, "win-win" interaction with technology, privacy cannot be *added on* to an ICT system after-the-fact, e.g., by adding a "compliance layer" on top of its core functionality to address relevant privacy legislation. Rather, in order to work in conjunction with technology and thus break the mold of zero-sum thinking, privacy must be proactively embedded into the design and architecture of an ICT system. This approach is able to address the growing challenges brought about by the increasing complexity of ICT systems, in a positive-sum, "win-win" manner, by addressing them at their source, by default—embedded in the architectural foundation of an ICT's operation.

The approach to privacy described above is embodied in the 7 Foundational Principles of *Privacy by Design*. In addressing the ever-increasing and systemic challenges of ICTs and networked systems, *Privacy by Design* provides a holistic, interdisciplinary framework. The application of *Privacy by Design* cuts across the entire structure of a business or organization, end-to-end, including its information technology, business practices and processes, physical design and networked infrastructure. It is in this way that it achieves a positive-sum, mutually beneficial interaction between privacy and technology.

The 7 Foundational Principles of *Privacy by Design* are as follows:

1. *Proactive* not Reactive; *Preventative* not Remedial

2. Privacy as the *Default Setting*

3. Privacy *Embedded* into Design

4. Full Functionality — *Positive-Sum*, not Zero-Sum

5. End-to-End Security — *Full Lifecycle Protection*

6. *Visibility* and *Transparency* — Keep it Open

7. *Respect* for User Privacy — Keep it *User-Centric*[5]

5 See Cavoukian, A. (2011). "*Privacy by Design*". The 7 Foundational Principles." Retrieved from http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

3. Foundational Principles of Security by Design

Information security seeks to enable and protect the activities and assets of both people and enterprises.

The NIST Glossary of Key Information Security Terms defines "Information Security" as: "Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

1) **integrity**, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

2) **confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

3) **availability**, which means ensuring timely and reliable access to and use of information."[6]

While information security has primarily been thought of as a defensive mechanism to protect enterprise activities and assets, we propose that properly implemented information security processes and technology can also be *enablers* for achieving business objectives.

For example, if a business has an objective to increase revenue by improving consumer satisfaction, then providing a secure environment to receive and manage consumer information as well as secure methods for granting access to such information can enhance customer confidence in the enterprise, leading to new revenue. The same is true when dealing with business partners or vendors.

A simple analogy poses the question: "Why do Formula 1 race cars have brakes?"

A traditional view would be: to make them stop (defensive posture). However, Formula 1 race cars have very sophisticated braking systems that allow them to go faster (enablement posture). NASCAR vehicles have a higher top speed than Formula 1 cars, appropriate for oval NASCAR race tracks, but Formula 1 cars will always beat NASCAR vehicles on the twists and turns of Formula 1 tracks because Formula 1 cars have better brakes.

Similarly, while the information security concepts of integrity and confidentiality can be thought of as defensive mechanisms (basic protection), the concept of availability can be thought of in more offensive terms (enabling business). As we seek to implement information security systems that both enable and protect enterprise activities and assets, we propose the 7 Foundational Principles of *Privacy by Design* be aligned with security in order to develop a Security by Design approach.

6 National Institute of Standards and Technology (2011). *Glossary of Key Information Security Terms*, ed. R. Kissel, p. 93. Retrieved from http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

By "Security by Design" we mean an approach to information security which, like *Privacy by Design*, is at once holistic, creative, anticipatory, interdisciplinary, robust, accountable and embedded into systems. It stands in direct contrast to "security through obscurity," which approaches security from the standpoints of secrecy, complexity or overall unintelligibility. Within the field of engineering, the approach of Security by Design has a lot in common with Ross Anderson's conception of "Security Engineering."[7]

Although in this paper we align work done in privacy (*Privacy by Design*) with security in order to develop an approach to security (Security by Design), it is important to note that the opposite has also taken place, i.e., work done in security has been aligned with privacy in order to further develop privacy. For example, the detailed approach taken by the NIST security risk assessment has been used to develop a more robust privacy impact statement.[8] Indeed, security risk assessments seek to address security issues early on in the development of an IT product, not after the fact. Thus their alignment with privacy impact statements can be said to be another example of the synergy between privacy and security "by design."

7 See Anderson, R (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Retrieved from http://www.cl.cam.ac.uk/~rja14/book.html

8 See Spiekermann, S., Oetzel, M. C. (2012), "Privacy-by-Design Through Systematic Privacy Impact Assessment – A Design Science Approach," ECIS - Conference Proceedings, 2012. Retrieved from http://ssrn.com/abstract=2050872

Privacy by Design and Security by Design

The following table illustrates, at a high level, how a set of Security by Design principles can be modeled upon the 7 Foundational Principles of *Privacy by Design*.

Privacy by Design **Foundational Principles**	**Privacy**	**Security**
	Respect and protect personal information.	Enable and protect activities and assets of both people and enterprises.
1. Proactive not Reactive; Preventative not Remedial	Anticipate and prevent privacy-invasive events *before* they happen. Do not wait for privacy risks to materialize.	Begin with the end in mind. Leverage enterprise architecture methods to guide the proactive implementation of security.
2. Default Setting	Build privacy measures directly into any given ICT system or business practice, by default.	Implement "Secure by Default" policies, including least privilege, need-to-know, least trust, mandatory access control and separation of duties.
3. Embedded into Design	Embed privacy into the design and architecture of ICT systems and business practices. Do not bolt it on after the fact.	Apply Software Security Assurance practices. Use hardware solutions such as Trusted Platform Module.
4. Positive-Sum	Accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a zero-sum approach involving unnecessary trade-offs.	Accommodate all stakeholders. Resolve conflicts to seek win-win.
5. End-to-End Security	Ensure cradle-to-grave, secure lifecycle management of information, end-to-end.	Ensure confidentiality, integrity and availability of all information for all stakeholders.
6. Visibility and Transparency	Keep component parts of IT systems and operations of business practices visible and transparent, to users and providers alike.	Strengthen security through open standards, well-known processes and external validation.
7. Respect for the User	Respect and protect interests of the individual, above all. Keep it user-centric.	Respect and protect the interests of all information owners. Security must accommodate both individual and enterprise interests.

Table 1 – Privacy by Design and Security by Design

Each of these Security by Design principles is explained in more detail below.

3.1 Proactive not Reactive; Preventative not Remedial

Many enterprises have historically responded to security threats in very reactive ways. But with security attacks increasing in frequency and sophistication, enterprises must build a security-minded culture and way of doing business that is much more proactive and preventative.

The following quotations emphasize the urgency of thinking in this way:

From the Verizon *2013 Data Breach Investigations Report*:

> Perhaps more so than any other year, the large scale and diverse nature of data breaches and other network attacks took center stage. [...] we witnessed separate, ongoing movements that seemed to come together in full crescendo throughout the year. And from pubs to public agencies, mom-and-pops to multinationals, nobody was immune. As a result—perhaps agitated by ancient Mayan doomsday predictions—a growing segment of the security community adopted an "assume you're breached" mentality.[9]

From *America the Vulnerable* by Joel Brenner:

> Companies must now reassess their risk postures and ask: What would happen if our basic designs, our formulas, or our codes were compromised? What would happen if our networks were taken down or corrupted? These are strategic risks, and organizations must do what well-managed organizations always do with risk: Buy it down.[10]

Preparing before the fact often requires a change in enterprise "state of mind" involving first, leadership and finally, the overall culture of the organization. This involves taking a strategic view, rather than responding to threats as they arise just with tactical actions. Borrowing advice from well-known business consultant Stephen R. Covey, we must "*Begin with the End in Mind.*"[11] While Dr. Covey's recommendation applies to creating a personal mission statement, the advice is equally compelling for enterprises. We need to take the strategic, proactive viewpoint, rather than the reactive, tactical one, defining what our security posture should be for an enterprise, and build upon that foundation.

We thus recommend that the discipline of enterprise architecture[12] (EA) be employed to proactively define an enterprise's security strategy. Gartner first applied this concept to information security in a 2006 paper entitled "Incorporating Security into the Enterprise Architecture Process."[13]

---

9 Verizon, 2013 *Data Breach Investigations Report*, p. 4. Retrieved from http://www.verizonenterprise.com/DBIR/2013/

10 Brenner, J. *America the Vulnerable. Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (Penguin Press HC, 2011).

11 Covey, S. R. "Habit 2: Begin with the End in Mind." *The 7 Habits of Highly Effective People*. Retrieved from https://www.stephencovey.com/7habits/7habits-habit2.php

12 See "Enterprise Architecture (EA)." *Gartner IT Glossary*. Retrieved from http://www.gartner.com/it-glossary/enterprise-architecture-ea/

13 Kreizman, G., Robertson, B. (2006). "Incorporating Security into the Enterprise Architecture Process." Retrieved from http://www.gartner.com/id=488575

Dr. Jeanne W. Ross, Director, Center for Information Systems Research, MIT Sloan School of Business, challenges enterprise leaders to build "a foundation for execution ... [with respect to] the IT infrastructure and digitized business processes automating a company's core capabilities."[14]

While enterprise architecture can span much more than information security, the methods employed by this discipline can enable an enterprise to define a holistic EA security strategy that becomes an integral part of an enterprise's "foundation for execution." Section 4 of this paper, "The Enterprise Security Journey," will outline an EA process for defining this strategy.

3.2 Secure by Default

Secure by Default is a concept that covers policies for implementing security controls and specific methods for installing and configuring software. In both cases, the goal is to make sure information systems are configured to be as secure as possible by default, rather than having users do it one by one or, worse, tightening down security after the fact.

In the software installation and configuration case, Secure by Default means that the initial setup or installation of a system contains a minimal set of software configured to the most secure settings as possible.

In the broader policy-driven view, Secure by Default requires that access to information, systems and applications be limited to just the data and functionality that are needed for a particular task.

Examples of such policies include:

- **Least Privilege**.[15] The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
- **Need-To-Know**.[16] A method of isolating information resources based on a user's need to have access to that resource in order to perform his/her job but no more. The terms "need-to-know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.
- **Least Trust**.[17] The principle that a security architecture should be designed in a way that minimizes 1) the number of components that require trust, and 2) the extent to which each component is trusted. The components should be distrusted by a secure architecture and designed in a fault-tolerant way.

14 Ross, J. W., *Enterprise Architecture as Strategy: Creating a Foundation for Business Execution.* (Cambridge, MA: Harvard Business Review Press, 2006).

15 National Institute of Standards and Technology (2011). *Glossary of Key Information Security Terms*, ed. R. Kissel, p. 110. Retrieved from http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

16 *Ibid* p. 125.

17 *Ibid* p. 111.

- **Mandatory Access Control**.[18] A means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals and need-to-know) of subjects to access information of such sensitivity.

- **Segregation of Duties.**[19] Separating certain areas of responsibility and duties in an effort to reduce fraud and unintentional mistakes. For example, an employee who accepts cash payments should not also be responsible for making bank deposits and reconciling bank statements.

This is an area where *Privacy by Design* and Security by Design show especially strong synergy. For example, the privacy principle of "data minimization" – collecting, using and exposing only the data elements needed to accomplish a specific task – is very much in line with the least privilege and need-to-know policies described above. Indeed, the application of data minimization may be enforced within an organization through security policies such as least privilege and need-to-know.

It should be noted that in many cases, strict policies of Secure by Default may conflict with Ease of Use objectives. Great care must be taken to build safeguards into the User Interface to allow users to easily access the information and functionality needed to complete their work, while preserving the fundamental concepts of Secure by Default.

3.3 Embedded into Design

In order to produce secure systems, security must be embedded into the design of such systems. Embedding security into the design of secure systems, however, can happen in two ways: through the *software* and through the *hardware* of a system. In this section we will first address the software side of embedding security into the design of secure systems through a discussion of "Software Security Assurance" followed by a discussion of the "Trusted Computing Module," which will address the hardware side of embedding security into the design of secure systems.

Software Security Assurance

Software Security Assurance has been defined as:

> The process of ensuring that software is designed to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources that it uses, controls, and protects.[20]

18 *Ibid* p. 116.

19 See "Separation of Duties." *Your Dictionary. Business.* Retrieved from http://business.yourdictionary.com/segregation-of-duties

20 "Software Security Assurance." *Wikipedia.* Retrieved from http://en.wikipedia.org/wiki/Software_security_assurance

Software Security Assurance seeks to decrease the risk of introducing security vulnerabilities at every step of the information system lifecycle, spanning definition, development, deployment and maintenance processes. To accomplish these objectives, privacy and security must be embedded into every standard, system, protocol and process.

A number of approaches to Software Security Assurance exist in the industry. Examples include the Software Assurance Maturity Model (SAMM)[21] and the Comprehensive, Lightweight Application Security Process (CLASP)[22]. An analysis of these approaches reveals the following basic practices:

- **Full Lifecycle Approach.** Security must be addressed throughout the full development of a software product: from requirements and design to implementation, testing and deployment. Security cannot be treated at one step only, as though it were simply a matter of building a defensive "perimeter" around a product. Rather, security must be considered at, and engineered into, every step of a product's lifecycle.

- **Comprehensive Threat Analysis**. The sensitivity of the data used by a product, the system processes that handle them and the potential repercussions from the loss, misuse or unauthorized access of any data must be assessed and prioritized. Misuse cases, data flows and data classification techniques should be used to determine the threat level of potential system breaches.

- **Security Built In to the System Architecture.** Security measures to address any potential threats must be designed into the architecture of the system, not bolted on after the fact. Security must be constructed as an essential component of the core functionality of the system.

- **Regular Code Review.** Exploitable flaws in the source code must be discovered through repeated code reviews and audits and fixed through recoding and/or redesigning of the system. Secure coding standards should be enforced and security modules should be designed for reuse.

- **Rigorous Security Testing.** The secure functionality of the system must be assured through structured testing and methods-based evaluation of the software features being delivered. Misuse cases should be tested against a live system and system "hacks" should be attempted.

For a discussion of Oracle's approach to Software Security Assurance, see Appendix A.

21 See the Software Assurance Maturity Model project website at http://www.opensamm.org

22 See Viega, J. "Building Security Requirements with CLASP." Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.124.9620&rep=rep1&type=pdf

Trusted Platform Module

The Trusted Platform Module (TPM) was developed by the Trusted Computing Group, an international industry standards group, as a technology used to shift the baseline of trust within a system from the software to the hardware. According to the EURIM Digital Policy Alliance white paper "Security by Design: Trusted Computing,"[23]

> TPMs provide hardware support for key management. They are computer chips (microcontrollers) with a finite storage capacity to store key material and certificates in a secure manner on the motherboard of computing devices and are based on open standards.[24]

Embedding key material and certificates into the hardware of a system allows data to be signed or hashed without the encryption key ever leaving the TPM. This protects the key from being changed or stolen by malware or other software-based threats, thus adding an additional layer of security to the cryptographic and authentication services of a system.

3.4 Positive-Sum, not Zero-Sum

Security by Design as with *Privacy by Design* seeks to achieve a positive-sum result where one can have both privacy *and* security. All too often privacy is forfeited for security. In addition to privacy, there are other objectives and interests that may appear to be in conflict with security. A few examples of conflicting objectives include:

- **Easy access vs. Secure access.** Business managers responsible for Business to Consumer sales over the Internet want to make it as easy as possible for customers to engage and buy something. Allowing a new customer to log in with her Facebook credentials makes it very easy for a customer to make an initial connection. However, the Facebook credentials may not be trustworthy enough to securely conduct a financial transaction.
- **Convenience vs. Security.** Most users hate passwords. They have too many online accounts and too many passwords. Therefore, it is very tempting to use simple passwords because they are convenient. However, experience has shown that this is very dangerous.
- **Simple to Implement vs. Secure to Use**. It is simpler and cheaper to implement an application that asks for all the data from a database record and presents that to the user than to selectively redact or expose individual data fields based on the user's role or level of responsibility. Also, it is often hard to design an application in a fault-tolerant way that can foresee all potential threats.

23 EURIM Digital Policy Alliance (2012). "Security by Design: Trusted Computing." Retrieved from http://dpalliance.org.uk/wp-content/uploads/2012/12/1112_Security-by-Design_Trusted_Computing.pdf

24 *Ibid* p. 5.

What can be done to achieve a positive-sum "win-win" outcome rather than an either-or situation? Here are some considerations from an enterprise perspective:

- **Seek to understand the objectives of all constituents.** Get all the issues on the table. Acknowledge that conflicts may exist and knowing what they are is the first step to resolution.
- **Evaluate potential conflicts.** Why do they exist? Are there ways to reframe expectations to minimize conflicts?
- **Understand current methods and technology.** Do the conflicts exist because of current limitations? Are there ways that existing technology or methods can be tweaked to minimize conflict?
- **Evaluate new methods and technology.** Are there new ways of doing things that would minimize or remove conflicts? What if we used new technology? Are there emerging technologies that will help us in the near future?
- **Seek effective compromise**. Are there ways we can adjust our expectations to accommodate conflicting objectives? Can we "meet in the middle" to resolve the conflict?
- **Implement trade-offs at the lowest level possible.** When a compromise is sought at a high level, it is usually one-dimensional, such as convenience vs. security, so that one wins at the cost of the other (zero-sum). On the other hand, trade-offs made at a low level create a multi-dimensional space where each individual component may have little effect on the final result but, taken together, they can bring the most optimal outcome (positive-sum).
- **Seek creative solutions.** Are there ways of (re)designing or (re)architecting the technology so that the conflict is resolved by being removed altogether? Sometimes a new perspective is all that is required.
- **Be willing to invest in effectiveness**. Sometimes, we will need to "bite the bullet" and invest more to get the results we need. Proper investment in new methods and technology may resolve conflicting objectives and deliver real business value.

3.5 End-to-End Security

The objective of enterprise security is to ensure confidentiality, integrity and availability of all information for all stakeholders in the enterprise. In order for it to really enable privacy, security must address and compensate for potential vulnerabilities throughout the enterprise, not just at the perimeter or in part of the enterprise. Experience has shown that old methods of protecting just the perimeter of the enterprise are woefully inadequate.

Only when the security strategy addresses the enterprise end-to-end can privacy be protected and enterprise activities and assets be enabled and protected.

Two key areas of information security, Database Security (DBSec) and Identity and Access Management (IAM), are vital to this discussion. While other information security controls are also important (e.g. network security, virus/malware protection), DBSec and IAM go right to the heart of privacy protection technology – protecting the information itself and securing access to that information.

Note that the following discussion provides only an overview of the benefits and functionality of DBSec and IAM. For a more detailed discussion of the benefits and technical capabilities of DBSec and IAM, see Appendix B.

Database Security

Information security requires that the confidentiality, integrity and availability of a database be protected. DBSec[25] has been defined as:

> a system or process by which the "Confidentiality, Integrity, and Availability," or CIA, of the database can be protected. Unauthorized entry or access to a database server signifies a loss of confidentiality; unauthorized alteration to the available data signifies loss of integrity; and lack of access to database services signifies loss of availability. Loss of one or more of these basic facets will have a significant impact on the security of the database.

This is best achieved through a two-pronged approach of:

- *Preventative Security Controls*, which proactively seek to prevent illegitimate actions from happening to data in the database; and
- *Detective Security Controls*, which monitor and analyze cases of illegitimate actions that do happen in the database.

Identity and Access Management

In addition to secure databases, information security requires that only appropriate access to information, systems and applications be granted. Gartner[26] defines IAM as:

> the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.
>
> IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. This security practice is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise.
>
> Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives.

25 "Database Security." *Bright Hub*. Retrieved from http://www.brighthub.com/computing/smb-security/articles/61400.aspx

26 "Identity and Access Management (IAM)." *Gartner IT Glossary*. Retrieved from http://www.gartner.com/it-glossary/identity-and-access-management-iam/

To achieve IAM, a system requires:

- *Identity Governance* functions, which ensure that the right people DO get access rights and the wrong people DON'T, provide knowledge of WHO has access to WHAT, disable access rights when people leave and enforce audit policies (ensure compliance);
- a *Directory Services* repository, which is the definitive, unified source for WHO has access and WHAT access they have; and
- *Access Management* mechanisms, so you automatically know WHO the user is (authentication), grant the RIGHT access (authorize) and enforce security policies (Web, mobile, cloud).

3.6 Visibility and Transparency

Visibility and transparency are well-known security principles that strengthen customer and vendor confidence in the security of information systems. Methods for providing such visibility and transparency include:

- **Open standards.** Well-known and highly vetted security standards should be employed. For example, using a well-known and extensively tested encryption standard like *Advanced Encryption Standard (AES)*[27] gives a high degree of confidence that encrypted data will be safe. On the other hand, new methods of encryption that are not as well known or tested may raise doubts about their security. In general, proprietary encryption algorithms should be avoided.
- **Well-known processes.** If a well-known process is followed for developing secure systems, users can be confident in the security of the system that is produced. Having a secure development process and using secure coding standards are examples of such processes.
- **External evaluation and validation.** Validation of security within a system may range from validation by current or prospective customers to formal validation according standard methods such as *FIPS 140-2*[28], a U.S. government computer security standard used to accredit cryptographic modules, or *Common Criteria*[29], an international standard (ISO/IEC 15408) for computer security certification.
- **Security policies.** Documenting and disclosing the constraints a security system may impose upon its users helps to ensure that a system is operating according to its stated promises and objectives. Accountability on the part of an organization does not detract from its business processes, but rather works to enable them.

27 See FIPS PUB 197 "Advanced Encryption Standard." Retrieved from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

28 See FIPS PUB 140-2 "Security Requirements for Cryptographic Modules." Retrieved from http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

29 See the Common Criteria project website at http://www.commoncriteriaportal.org/

3.7 Respect for the User

A basic principle of *Privacy by Design* is to focus on the individual and have respect for individual privacy rights. Security, however, addresses a broader constituency. It must respect and protect the interests of all information owners, accommodating both individual and enterprise interests.

For example, economic espionage, where the primary target is intellectual property, not personally identifiable information (PII), is rampant in today's business environment. In such cases, the need to protect enterprise data is paramount. In his book *America the Vulnerable*, Joel Brenner states:

> The level of Internet crime is staggering. Our companies and government are under relentless cyber assault twenty-four hours a day, and they are bleeding – we are bleeding – military secrets, commercial secrets, and technology that drive our standard of living and create our power as a nation. The astounding advances in the electronic processing and storage of information that have given us so much wealth and pleasure have also left us nearly defenseless against endemic crime and systematic espionage by foreign intelligence services, criminal gangs, and unscrupulous competitors. Much of the crime originates in Eastern Europe and Nigeria. The most persistent espionage – particularly economic espionage – originates in China.[30]

Although security addresses a broader constituency than privacy, privacy principles are nonetheless essential in order to keep the interests of individuals separate from those of enterprises. For example, a company whose employees may also be its customers (e.g. financial services firm) may be tempted to use employee data it obtained under one relationship (employer-employee) to enhance its ability to sell goods or services in the other relationship (vendor-customer). Here, privacy principles such as data minimization and purpose specification should be leveraged to separate those conflicting interests. These privacy principles, in turn, should be enforced within an enterprise through security policies such as segregation of duties, least privilege and need-to-know.

30 Brenner, J. *America the Vulnerable. Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (Penguin Press HC, 2011).

4. The Enterprise Security Journey

It is not simply by chance that, of the 7 Foundational Principles of *Privacy by Design* and by extension Security by Design, the first is "*Proactive* not Reactive; *Preventative* not Remedial." In order to become a reality, these "by design" principles require, above all, leadership and goal-setting. Leadership and goal-setting are abilities which occur not at the level of technology or legislation, but rather at the level of business practices. Thus in order to implement a "by design" approach to privacy or security, what is first and foremost required is a strategic, proactive viewpoint within an organization, rather than a reactive, tactical one based on compliance.

Taking our lead from this first, all-important principle, in this section we will build upon the Security by Design principles defined in the previous section and develop an enterprise-level process for defining, governing and realizing a Security by Design approach.

Enterprise security is a journey, not a single project or disjointed set of loosely related projects. A successful enterprise security strategy provides an umbrella vision of what a company wants to achieve, an orderly plan for how to enable and protect that objective and an approach to governing the process.

This section addresses these three key areas:

- Enterprise Architecture Approach to Security
- Charting the Security Course
- Guiding the Journey

4.1 Enterprise Architecture Approach to Security

In section 3.1 ("Proactive not Reactive; Preventative not Remedial"), we introduced how enterprise architecture (EA) can be applied to define a holistic information security strategy that becomes an integral part of an enterprise's "foundation for execution." With such an umbrella security strategy in place, an enterprise can be proactive, rather than reactive, in addressing security concerns. Investment in security technology and processes can be aligned with what the business is trying to accomplish, rather than just focusing on what technology can do.

Since the first Zachman Framework in 1987, many EA frameworks have been developed with the goal of enabling an enterprise to align its IT infrastructure with business objectives. In addition to the Zachman Enterprise Framework, other examples include The Open Group Architecture Framework (TOGAF), OMG Federal Enterprise Architecture (FEA), and The Gartner Methodology (formerly the Meta Framework). Each framework comes with its various strengths and weaknesses depending on the enterprise to which it is applied.

The Oracle Enterprise Architecture Framework[31] is a hybrid EA framework influenced by TOGAF, FEA and Gartner and has clear mappings to both TOGAF and FEA, which allows its users to switch easily to other EA frameworks if they so choose.

This section briefly explains how this framework can be applied to develop a holistic information security strategy. Figure 1 outlines the six primary components that make up this framework.

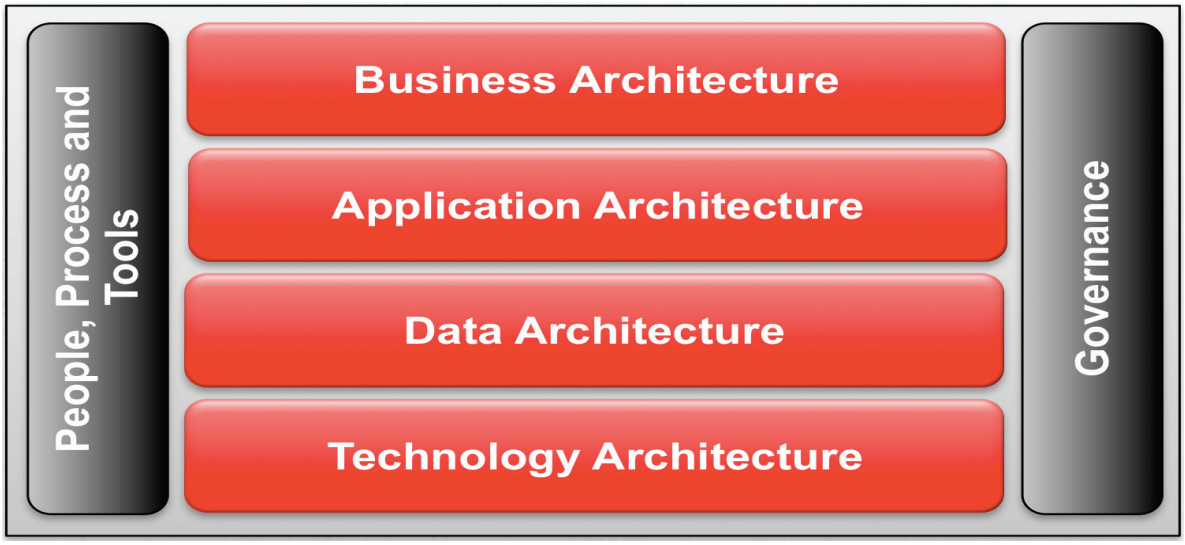

Figure 1 – Oracle Enterprise Architecture Framework

Business Architecture

Any security architectural discussion should begin with business architecture. This business architecture allows us to understand what must be enabled and protected in order to achieve desired business results.

The business architecture aligns an organization's operating model, strategies and objectives with IT. It also provides a foundation for developing a business case for IT transformations. If security is to enable and protect the business, investments in security must align with business objectives and strategies.

The business architecture also provides a business-centric view of the enterprise from a functional perspective. This business-centric view includes business objectives (what we want to accomplish), strategy (how we intend to achieve those objectives), functions (critical functions necessary to implement the strategy) and organization (who the key leaders are and how they relate to each other).

This is the level at which leadership and goal-setting with respect to security occurs. If security is not a priority at the highest level of a business or organization, security objectives and a functional strategy to carry them out will not spread throughout an enterprise's operations.

31 See "The Oracle Enterprise Architecture Framework," p. 4. Retrieved from http://www.oracle.com/technetwork/topics/entarch/oea-framework-133702.pdf

The same holds true for the case of implementing *Privacy by Design* at the enterprise level. Leadership and goal-setting at the highest levels of an organization are required in order to prescribe and enforce high standards of privacy and data protection, and go beyond compliance with legislation. A preventative and systematic approach to engineering privacy and data protection requires a clear commitment in terms of business objectives, strategy and functions within an organization.

Application Architecture

The application architecture provides an application- and services-centric view of an organization that ties business functions and services to application processes, services and components in alignment with the application strategy. Identifying key application functionality allows us to define what security measures are essential to enable and protect an organization's assets.

For example, identifying the essential corporate applications that must access and use credit card information allows us to focus on which applications and related data sets must be secured according the PCI DSS standards.[32] This would enable us to embed a well-established security standard into the design of application processes, services and components, thus achieving a combined application of the principles of "Embedded into Design" (section 3.3) and "Visibility and Transparency" (section 3.6).

In the case of implementing *Privacy by Design* at the enterprise level, the application architecture is the organizational level where considerations about how privacy can be embedded into the design and architecture of IT systems and business practices should occur. A systematic, principled approach to embedding privacy and data protections should be adopted, relying upon accepted standards and process frameworks. Detailed privacy impact and risk assessments should be carried out in order to mitigate privacy risks and consider alternatives. Similar to the example discussed above, this is where the principles of "Privacy Embedded into Design" and "Visibility and Transparency" should be realized.

Information Architecture

The information architecture describes all of the moving pieces and parts for managing information across the enterprise, and the sharing of that information with the right people at the right time to realize the business objectives stated in the business architecture.

Identifying key data sets that must be protected to achieve privacy objectives and other regulatory requirements is a critical part of the information architecture (although an enterprise must also recognize that data protection includes other privacy objectives such as use limitation and purpose specification). Understanding the relative value of different types of information is critical. Being able to assess the risk an organization faces if key data are compromised or lost is necessary to prioritize investment in security infrastructure and processes.

32 See the PCI SSC Data Security Standards website at https://www.pcisecuritystandards.org/security_standards/index.php

For example, identifying key data sets that must be protected allows us to focus on and determine the right security policies for that data. Applying the principle of "Secure by Default" (section 3.2), these would include policies such as Least Privilege, Need-To-Know, Least Trust, Mandatory Access Control and Segregation of Duties.

In the case of implementing *Privacy by Design* at the enterprise level, the information architecture of an organization is where considerations regarding data minimization and purpose specification should occur and the principle of "Privacy by Default" be realized. Understanding how much personally identifiable information (PII) is needed in order to carry out a business objective is key to collecting, using and disclosing *only* that amount within an application. In addition, the length of time PII is needed and used by an enterprise for a particular business objective should be evaluated and determined. Once PII is no longer needed by an application or process, it should be securely destroyed.

Technology Architecture

The technology architecture describes how the infrastructure underlying the business, application and information architectures is organized. In this way, the technology architecture becomes an enabler for the business, the "foundation for execution" that will make it possible for the business to achieve its objectives.

Unfortunately, when technology solutions are implemented without strong alignment with business objectives, investment of time and money is wasted, and meaningful objectives may never be realized.

However, correct alignment of technology with business objectives can allow the business to leverage technology as a competitive differentiator and accelerator of business success.

For example, suppose a business has major objectives to improve supply chain efficiency and increase customer satisfaction. If a good IAM architecture is implemented internally within the enterprise, but IAM infrastructure to support external users (e.g. customers, suppliers and partners) is not provided, the critical corporate supply chain and sales objectives will suffer, even though internal users are well-served and happy. Focusing the technology (in this case, IAM functionality) where the business is focused (supply chain and customers) would deliver stronger results, thus achieving the principle of "End-to-End Security" (section 3.5) where it is most needed within a business.

Similarly in the case of implementing *Privacy by Design* at the enterprise level, the EA component of technology architecture is where the principle of "End-to-End Security" should be realized. Understanding what security measures are needed in order to protect PII throughout its lifecycle is essential to choosing the right technology and networked infrastructure within a business.

People, Process and Tools

This area of the framework identifies the people, processes and tools used to define enterprise architectures and architecture solutions. It must be recognized that technology alone seldom achieves desired results. It is how people work with the technology that delivers results.

Consider a simple example. We know that encryption is a necessary technology to implement strong privacy protection for the PII required by an enterprise. However, if the wrong data elements are encrypted, neither privacy nor security objectives will be achieved, leaving the enterprise open to potential data breaches or regulatory violations. It is how the technology is used, not the technology itself, that delivers the needed protection. In this example, proper use of the technology requires that the interests of the end-user be kept uppermost. Thus the principle of "Respect" (section 3.7) for all information owners must be applied.

In the case of implementing *Privacy by Design* at the enterprise level, the area of people, process and tools is where considerations regarding user-centricity should occur and the principle of "Respect for User Privacy" be realized. Awarding the interests of the individual the highest priority is how the right enterprise decisions regarding informed consent, accuracy of information and redress are made.

Governance

EA governance provides the structure and processes for making sure that technology solutions continue to be aligned with enterprise objectives. It is not enough to create an initial security strategy without implementing governance processes that will help make it a reality. Successful governance processes include people, processes, policies, technology and finance.

By its very nature, security impacts all facets of an organization. Consequently, representative stakeholders from the different parts of the organization must be involved in the governance process. This requires the culture of an organization to be one in which representative stakeholders take a leading, proactive role with respect to security, rather than viewing security as someone else's responsibility. Thinking of security in terms of "zero-sum" trade-offs of responsibility within an organization will no longer work. Successful governance processes for security require a "positive-sum" model of cross-departmental leadership.

In the case of implementing *Privacy by Design* at the enterprise level, understanding all the interests and objectives throughout an enterprise is key to embedding privacy and data protection into applications or processes such that their requirements are optimized and all legitimate interests are accommodated. This requires EA governance in a manner consistent with the principle of "Full Functionality – Positive-Sum, not Zero-Sum."

4.2 Charting the Security Course

The following steps can be followed to create an EA security strategy using the framework described above.

- **Understand Business Objectives and Strategies**. The first step in creating an EA security strategy is to understand what the business wants to do. We must answer fundamental questions about the business such as: What are the business objectives? What is the enterprise's operating model (how it does business)? What is the strategy for achieving success? How can we measure success? What regulatory requirements must we meet? By understanding business objectives and strategies first, we can focus on what is necessary

to enable the business, not just on what technologies are available or nice to have. Technology architectures can then have real meaning in business terms, offering real value to the enterprise.

- **Assess Current State – Where you Are Now.** The Current State defines both the structure and outcomes of the current security architecture. Are we currently taking a piecemeal, reactive, tactical approach to security, or do we have an orderly, structured, strategic plan for achieving our security objectives? Are our current security initiatives aligned with business objectives? What systems and processes do we have in place? How well are they working? What are our strengths? What are our weaknesses? What risks do we face? Do we have any current, observed or measurable evidence that indicates the effectiveness of our current plans and infrastructure? How mature is our approach to security, relative to other organizations in our market?

Ranking the current state according to a Security Capability Maturity Model,[33] such as the one briefly outlined below, can be helpful in determining how well the enterprise is doing with its security posture.

Maturity Level	Approach	Platform Characteristics
1	Reactive	• Primarily manual methods. • Little automation. • Processes are ad-hoc and disorganized. • Limited awareness or acceptance across the organization.
2	Tactical	• Diverse mix of manual methods and automated systems. • A few individual advocates exist. • Repeatable processes are beginning to be established.
3	Strategic	• Unified architecture established. • Management buy-in is secured. • Gaps are identified. • Implementation progressing well according to well-defined plan.
4	Enterprise	• Unified architecture in place for key business units. • High value applications, systems and databases are covered. • Processes are becoming and integral part of the culture. • Performance is highly predictable.
5	Continuous Improvement	• Unified architecture in place for all business units. • Processes are mature and being optimized. • All applications, systems and databases are covered.

Figure 2 – Security Capability Maturity Model

- **Define Future State – Where you Want to Be.** Defining the desired Future State is the same as mentally looking into the future and defining what you want to achieve by a particular time. Using the Enterprise Architecture framework, we can document answers to questions such as: What levels of security do I need to enable and protect my business objectives? What applications and data need to be protected? What technology and processes need to be in place? How will I measure effectiveness? How will new security measures affect stakeholders?

33 See "What is the Capability Maturity Model? (CMM)." *Select Business Solutions*. Retrieved from http://www.selectbs.com/process-maturity/what-is-the-capability-maturity-model

A Security Capability Maturity Model such as the one shown in Figure 2 can also be helpful in determining the level of maturity an enterprise wants to achieve in its Future State.

- **Evaluate Gaps.** Evaluating gaps is the process of comparing Current State with Future State and determining what is necessary to get us from where we are to where we want to be. What technology solutions are we missing altogether? What existing systems need to be improved? Are our security processes and procedures up to date with current threats? Are there things we are doing now that don't align with business objectives? Are our critical processes adequately supported by technology? Since we probably can't solve all challenges at once, what issues are most important? How can we prioritize our needs and investment?

  By defining which gaps exist between the Current State and Future State, we can intelligently determine what steps need to be taken to achieve Future State objectives.

- **Define the Enabling Architecture**. The technology architecture which enables and protects business assets and actions must be firmly aligned with the business, application and data architecture layers in the Enterprise Architecture model. What specific technologies do we need? How must they work together? What standards should be employed? What is available from existing vendors? What unique requirements does our enterprise have that might demand custom development? What can we learn from other companies in the market? Will this technology infrastructure accommodate anticipated growth and changes in our enterprise?

  Up to this point, nearly all of our discussion has defined architecture in terms of capabilities, rather than specific technology solutions. However, defining the enabling architecture might require that technology choices be made. For example, if the Current State shows a highly diverse set of directory technologies, and the Future State architecture calls for a consolidated infrastructure to improve performance, decrease cost and improve reliability, the Enabling Architecture might get quite specific on what type of directory meets this need for consolidation.

- **Define the Strategic Roadmap**. Rarely can all security challenges be addressed immediately. We must make tough decisions and lay out a strategic sequence for implementing a security strategy. What is most important to our enterprise? What are our biggest risks that demand attention? Where should we start? Can investment in foundation infrastructure now make our life simpler in the future? How can we move from our current technology environment to where we need to be? Should we make big wholesale changes, or does a more incremental approach fit us best? What deadlines must we meet to properly support business schedules?

  The Strategic Roadmap is typically not a detailed project plan, but shows major priorities and sequence of activities. It will highlight major dependencies that may exist between system elements or scheduled business events.

- **Define the Business Case.** Defining a business case for security initiatives can be challenging. Certainly, traditional return on investment (ROI) calculations can show measureable benefits for some parts of the infrastructure, but in other cases, benefits of security solutions are measured in terms of risk mitigation or avoidance. However, evaluating several benefits areas, including both risk mitigation/avoidance and ROI estimates, can produce a comprehensive business case to justify investment. We should answer questions such as: What security risks exist for our enterprise? What impact would we feel from loss of data or misuse of data? What would be the direct cost to compensate for a data breach? How would our brand be damaged? What about loss of customer confidence in our company? Where can good security influence revenue positively? What security solutions can be justified by ROI?

  An example of an innovative approach to justifying investment in security infrastructure is described in the Securosis white paper, "The Business Justification for Data Security."[34] This method uses a five-step process illustrated in the following diagram for compiling a comprehensive set of benefits that could accrue from a specific security investment.

Figure 3 - The Business Justification for Data Security

- **Define the Governance Process.** The best security strategy is of little use unless it leads to action and results. A strong governance process is necessary to make sure the technology solutions remain firmly aligned with business objectives, progress is being made according to plan and stakeholder expectations are being met. To establish the appropriate governance process, we should answer questions such as: Who are our key stakeholders? What are their expectations? How can we organize to provide adequate representation from critical stakeholder groups? How can we effectively communicate? How will we measure progress and success? How will we adapt to changing conditions?

4.3 Guiding the Journey

Implementing an EA security strategy is a long-term process, not a short-term project. It evolves over time and must be flexible enough to adjust to changing market conditions, strategy shifts, new innovations in technology and new threats from the "bad guys." Therefore, it is critical to outline a governance process to guide and govern the journey.

34 Securosis, L.L.C., The Sans Institute (2009). "The Business Justification for Data Security." Retrieved from https://securosis.com/assets/library/reports/TheBusinessJustificationForDataSecurityV10.pdf

Defining the governance process is an integral part of the enterprise security architecture, as explained in the previous section. However, a successful governance process should include more than the process definition. These five guidelines can be useful in both defining and executing the governance process:

- **Secure executive sponsorship and commitment.** An enterprise security strategy must not be an IT-only initiative. This strategy must be sponsored by, and have the commitment of, the top ranking officers in the organization. Full executive commitment to security is often difficult to secure, but is essential for success. Without such commitment, appropriate funding may not be available to do what is needed, consistent attention to critical security issues may lapse and appropriate management and technical people may be diverted to other issues. Unfortunately, it too often takes a major, public data breach before executives give the proper strategic attention to security.

- **Align all stakeholders to support enterprise objectives.** Because of the wide variety of stakeholders affected by an enterprise security strategy, it is essential to align these stakeholders behind a set of well-understood objectives. This includes vertical alignment within an organization, from executives to project participants, but also horizontal alignment – across departmental boundaries within an organization and extending outward to include technology vendors and systems integrators, as needed. Identifying all these stakeholders, defining roles and establishing alignment linkages between them can be very helpful.

- **Establish and conduct an effective communications plan among constituents**. Once stakeholders are properly aligned, an appropriate schedule of communication should be established, both for routine project and program communications as well as escalation procedures, both within the organization and with external parties. In many cases, good communication is the single largest contributor to project success.

- **Establish and execute a follow-up cadence at all levels**. Having a plan is not enough. It must be consistently followed. Having a prescribed cadence for different levels of stakeholders is important. For example, weekly meetings for key project people, monthly governance council reviews and quarterly executive reviews may be in order. These should include appropriate external participants (e.g. software vendor, systems integrator) as required. Remember, consistency is key.

- **Develop performance metrics and evaluate effectiveness of enterprise decisions.** An enterprise security strategy should promote and produce effective enterprise decisions on issues relating to the alignment of IT infrastructure with business objectives. In order to ensure that effective enterprise decisions are being made, metrics should be developed to measure the use of enterprise security strategies in making decisions about IT investment, their effectiveness within the overall decision-making process and the quality of the decisions made using them.

This governance process is a basic approach that has been proven to be effective many times. However, this process is too frequently ignored or taken too lightly. Unfortunately, lapses in follow-through or improper attention to details at the right time in the lifecycle of an initiative often cause misunderstandings, project delays and cost overruns, making it tough to appropriately support business objectives. When this process is taken seriously, however, it provides the flexible leadership required for an enterprise to adjust to changes in markets, strategies and technologies. In the case of implementing an EA security strategy with Security by Design, it guides an enterprise towards taking proactive, rather than reactive, measures in addressing security concerns. The same holds true for an EA privacy strategy with *Privacy by Design*, albeit here the governance process guides an enterprise towards being proactive rather than reactive with respect to addressing privacy concerns.

Conclusion

In this paper, we explored the strong synergy that exists between the related disciplines of privacy and security. While on the one hand, strong security is essential to meet the objectives of privacy, on the other hand, well-known privacy principles are valuable in guiding the implementation of security systems. On the basis of this synergy, we defined a set of foundational principles for Security by Design that are modeled upon and support the foundational principles of *Privacy by Design*. These new Security by Design principles show how the 7 Foundational Principles of *Privacy by Design* should ideally be followed to also develop a Security by Design approach, through measures such as:

- Proactive and Preventative, not Reactive and Remedial
- Secure by Default
- Security Embedded into Design
- Positive-Sum, not Zero-Sum
- End-to-End Security
- Visibility and Transparency
- Respect for the User

On the basis of this new Security by Design approach, we then developed an enterprise-level process for defining, governing and realizing a "by design" approach to security. In order to become a reality for enterprises, Security by Design requires strong leadership, continuous goal-setting and consistent follow-through. Enterprise Architecture is an ongoing journey, not a single project or disjointed set of loosely related projects. Our discussion found that if an EA framework is followed to define an EA security strategy in harmony with the holistic, interdisciplinary principles of *Privacy by Design* and Security by Design, and if a formal governance process is implemented to guide and govern the journey, then an enterprise can indeed be proactive, rather than reactive, in addressing any security concerns. This will lead to stronger security, and better privacy, for all – a positive-sum, win-win proposition!

Appendix A: Oracle Software Security Assurance

This appendix supplements the discussion of Software Security Assurance found in section 3.3 "Embedded into Design." It discusses the basic practices used in Oracle's approach to Software Security Assurance to illustrate a successful approach to embedding security in a large, diverse product portfolio.

Oracle Corporation follows Software Security Assurance methods for building security into the design, build, testing and maintenance of its products by adhering to the following basic principles:[35]

- **A Lifecycle Approach to Security.** Focused attention on security is included throughout the various phases of the life of a product: from design and development to release and maintenance. While the product development phase is the one in which most of Software Security Assurance activities are focused, Software Security Assurance activities also extend to the ongoing maintenance of products after they have been released to customers.

- **System Definition.** Good security needs to be built in, not bolted on, to a product. Secure development starts early in the product definition phase and continues through the entire product lifecycle. Security requirements are gathered and documented early in the design stage based on two principles: 1) Consistency—New features should have consistent security behavior when compared to other product features and 2) Simplicity—A feature should not introduce a new privilege model where there is an existing privilege model unless there is an outstanding reason to do so.

- **Common Security Modules.** Some problems are best solved only once. Development teams can benefit from common security modules that save time because each team does not have to track down the kinds of subtle errors that creep into certain core features. Critical security functionality is consolidated into core modules and services are tested extensively for use across many products.

- **Independent Validation.** Selected customers are engaged to validate and gather additional feedback and guidance on matters relating to the security of products. Such customer feedback helps assure that the technology is not only secure, but that processes and procedures are in place to support security in the products over their lifetime.

- **System Development and Deployment.** Following Secure Coding Standards[36] assures that lessons learned from past experience are followed in building the products. Ongoing reviews by product teams continue to validate compliance with Secure Coding Standards and previously documented security specifications.

35 See "Oracle Software Security Assurance." *Oracle*. Retrieved from http://www.oracle.com/us/support/assurance/index.html

36 See "Secure Coding Standards." *Oracle*. Retrieved from http://www.oracle.com/us/support/assurance/coding/index.html

- **Security Analysis and Testing.** Extensive use of testing tools by both Development and Quality Assurance teams provides ongoing feedback on the quality of the code produced during the development phase before the final product is shipped.
- **Security Assessments.** Security assessments, also called ethical hacking, consist of security testing using a structured, methodical approach carried out against an Oracle product. A security assessment looks at product architecture from a security perspective, identifies security bugs, and documents them. The goal is to identify vulnerabilities as well as to educate the development group on secure coding techniques that can be applied going forward.

Appendix B: End-to-End Security

This appendix supplements the discussion of end-to-end security in section 3.5. It is a more detailed discussion of the benefits and technical capabilities of Database Security and Information and Access Management with respect to developing a Security by Design approach.

B.1 Database Security

Information is the heart and soul of modern business. Proper use of data enables businesses to thrive. Misuse or loss of that information can have the opposite effect.

Database Security[37] (DBSec) has been defined as:

> a system or process by which the "Confidentiality, Integrity, and Availability," or CIA, of the database can be protected. Unauthorized entry or access to a database server signifies a loss of confidentiality; unauthorized alteration to the available data signifies loss of integrity; and lack of access to database services signifies loss of availability. Loss of one or more of these basic facets will have a significant impact on the security of the database.

The following simple model highlights both Preventative and Detective security controls recommended to secure relational databases.

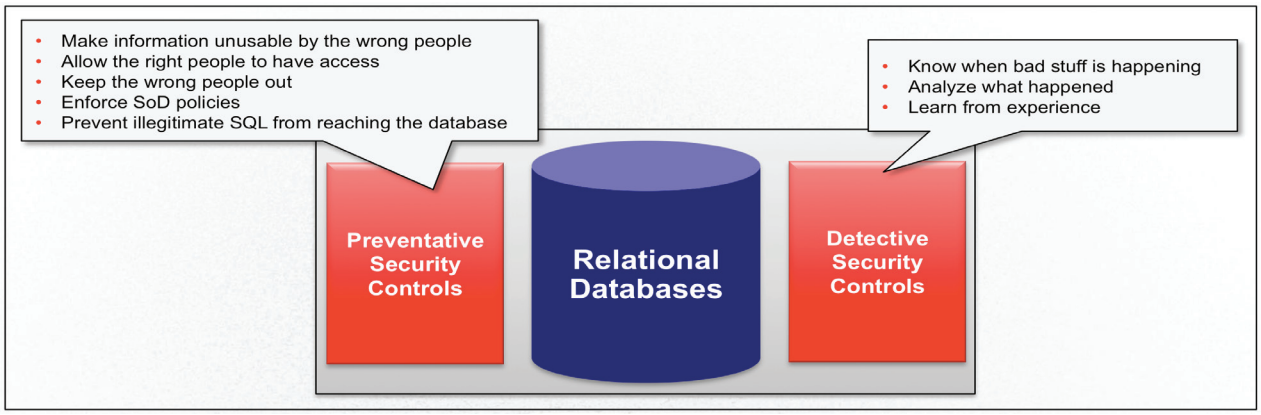

Figure 4 – DBSec Business Benefits

Preventative Security Controls shown in Figure 4 are proactive measures to prevent illegitimate actions from happening to data in the database. Business benefits from such controls include:

- Make information unusable by the wrong people.
- Allow the right people to have access.
- Keep the wrong people out.

37 "Database Security." *Bright Hub*. Retrieved from http://www.brighthub.com/computing/smb-security/articles/61400.aspx

- Enforce Segregation of Duties (SoD) policies.
- Prevent illegitimate SQL from reaching the database.

On the other hand, **Detective Security Controls** are used to monitor and analyze the cases when illegitimate actions do happen in the database. Benefits include:

- Know when bad actions are happening.
- Analyze what happened.
- Learn from experience.

Figure 5 illustrates the functional capabilities of DBSec – the actual security controls – that are necessary to deliver these benefits.

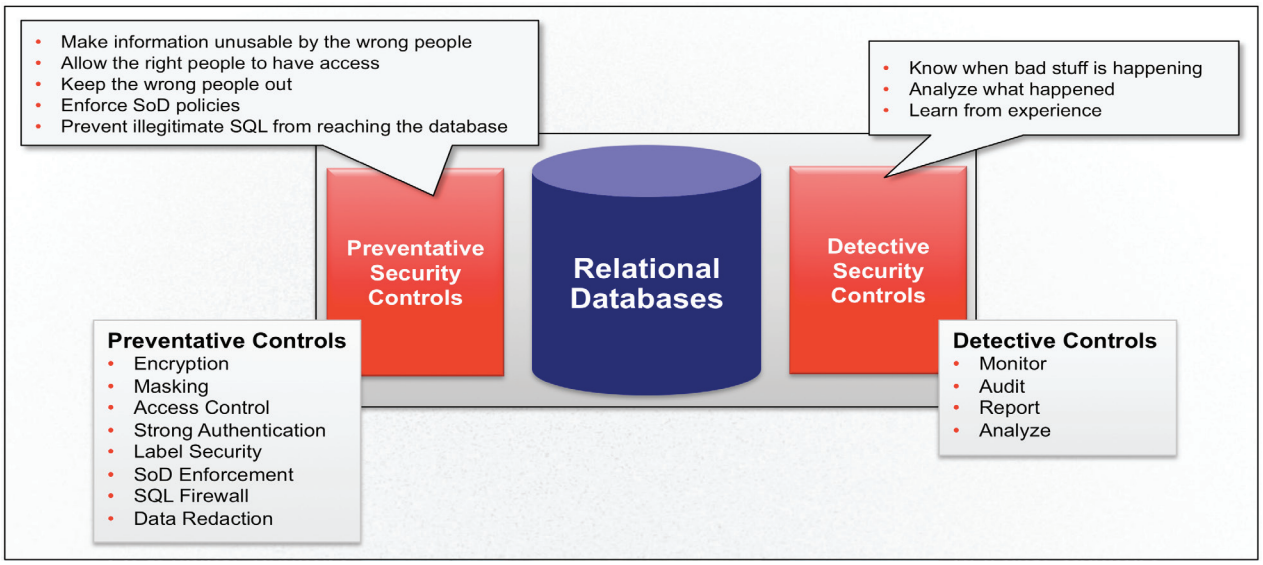

Figure 5 – DBSec Security Controls

Preventative Security Controls include the following functional capabilities:

- **Encryption.** Encrypt sensitive data sets or specific sensitive columns, such as credit cards, social security numbers or personally identifiable information (PII) – at rest or in transit.
- **Masking**. Replace sensitive information such as credit card or social security numbers with realistic values to accommodate testing, without exposing sensitive data to non-authorized users.
- **Access Control**. Allow only authorized users to access the database.
- **Strong Authentication**. Provide multi-factor user authentication, and other strong authentication methods including support for such methods as PKI, Kerberos and RADIUS.
- **Label Security**. Manage access to data on a "need to know" basis in order to protect data privacy and achieve regulatory compliance.

- **SoD Enforcement**. Increase the security of existing applications and address regulatory mandates that call for segregation of duties, least privilege and other preventive controls to ensure data integrity and data privacy.
- **SQL Firewall**. This firewall acts as a first line of defense - transparently detecting and blocking SQL injection attacks, privilege escalation and other threats against relational databases.
- **Data Redaction**. Limit data actually delivered from the database to a requesting application, depending on user roles and access privileges. This can be instrumental in achieving the Data Minimization objective required by privacy, although by the same token the database should itself contain only the information required to carry out the purpose of the technology accessing it.

Detective Security Controls include the following functional capabilities:

- **Monitor**. Automatically detects unauthorized database activities that violate security policies, and thwarts perpetrators from covering their tracks.
- **Audit**. Consolidates audit data and logs generated by databases, operating systems, directories, file systems and custom sources into a secure centralized repository.
- **Report**. Provides enterprise security intelligence and efficient compliance reporting by combining monitoring and audit data.
- **Analyze**. Analyzes audit and event data and takes action in a timely manner.

B.2 Identity and Access Management

Identity and Access Management (IAM) is focused on managing user access to information, systems and applications in an orderly, controlled fashion.

Gartner[38] defines IAM as:

> the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.
>
> IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. This security practice is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise.
>
> Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives.

Figure 6 illustrates the basic benefits IAM offers to enterprises.

38 "Identity and Access Management (IAM)." *Gartner IT Glossary*. Retrieved from http://www.gartner.com/it-glossary/identity-and-access-management-iam/

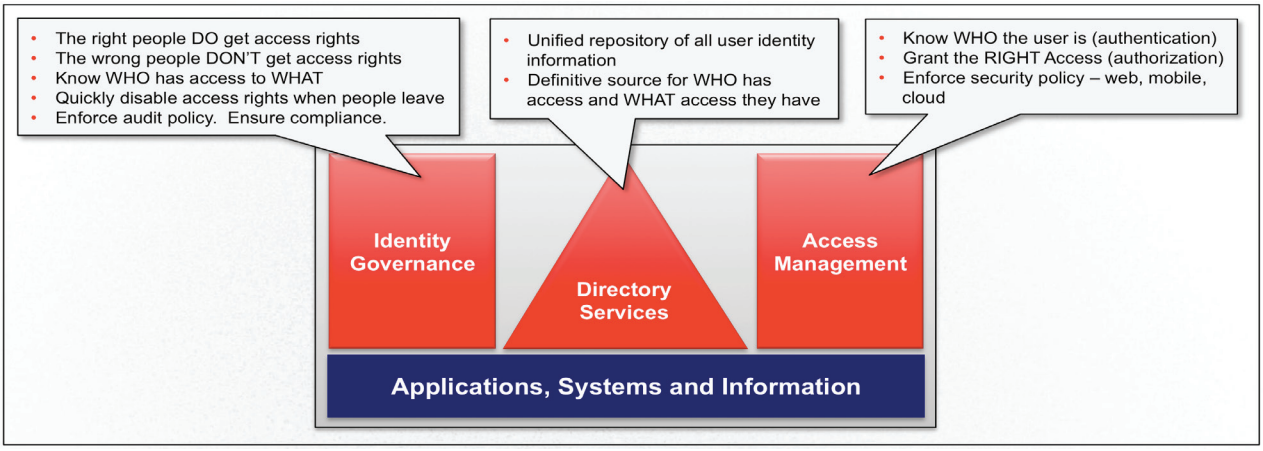

Figure 6 - IAM Business Benefits

Identity Governance functions depicted in Figure 6 provide the administrative capabilities to ensure that:

- The right people DO get access rights.
- The wrong people DON'T get access rights.
- Know WHO has access to WHAT.
- Quickly disable access rights when people leave.
- Enforce audit policy. Ensure compliance.

Directory Services provide definitive repositories of user identity and access rights information:

- Unified repository of all user identity information.
- Definitive source for WHO has access and WHAT access they have.

Access Management provides the mechanisms to enforce security policies at the time users attempt to access applications, systems or databases, so you automatically:

- Know WHO the user is (authentication).
- Grant the RIGHT Access (authorization).
- Enforce security policy – web, mobile, cloud.

Figure 7 illustrates the functional capabilities of Identity and Access Management necessary to deliver these benefits

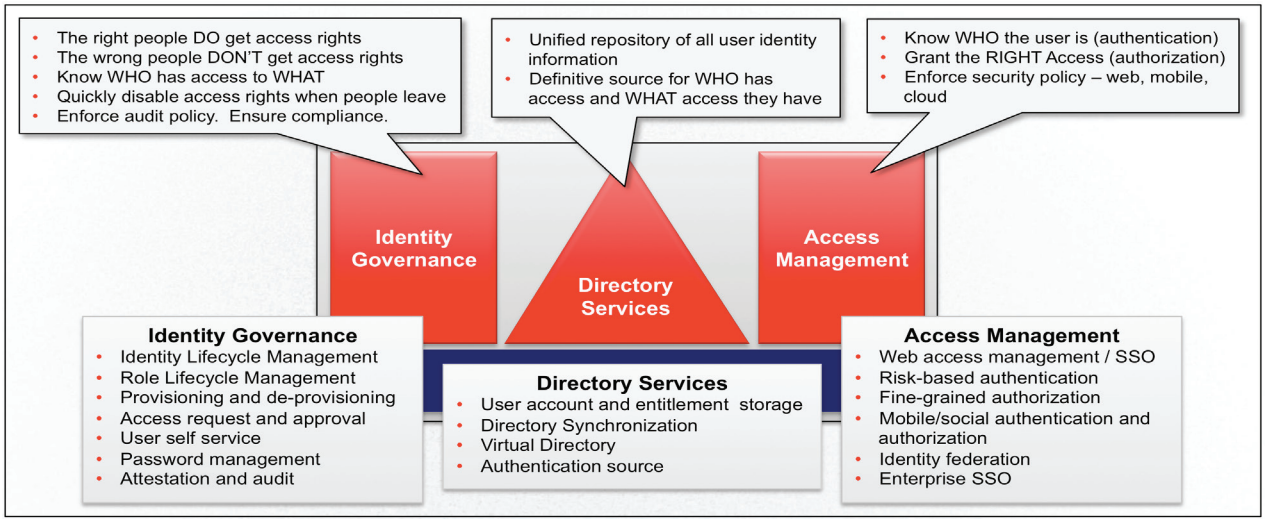

Figure 7 – IAM Technical Capabilities

Identity Governance technical capabilities include:

- **Identity Lifecycle Management**. Managing the complete lifecycle of identities and access rights for users, from on-boarding, changes in responsibilities and off-boarding.
- **Role Lifecycle Management**. Managing the complete lifecycle of user roles, including role discovery, definition, ownership, changes and retirement.
- **Provisioning and de-provisioning**. Enabling, changing, disabling and removing users, accounts and access rights on target applications, systems and databases.
- **Access request and approval**. The ability for users to easily request access rights (e.g. roles or entitlements) and have managers or data owners approve such access rights.
- **User self-service**. The ability of users to self-register, request access rights, manage passwords and other personal information and complete delegated administration tasks.
- **Password management**. The ability to specify and enforce password policies, including password complexity and password reset schedule.
- **Attestation and audit**. Automated audit policy enforcement, audit data analytics and automated support for periodic attestation or certification of users and their access rights.

Directory Services technical capabilities include:

- **User account and entitlement storage**. A unified repository for all user identity and access rights information.
- **Directory Synchronization**. Synchronization among multiple directory instances for performance or fault-tolerance purposes.

- **Virtual Directory**. A unified identity service to provide a single LDAP access point by aggregating data from several data repositories (e.g., directories, databases) without physically consolidating such repositories.

- **Authentication source**. Providing a definitive, centrally managed source for authenticating users of applications, databases and operating systems.

Access Management capabilities include:

- **Web access management / Single sign-on (SSO)**. Mechanisms for providing standardized authentication, session management and policy enforcement methods to provide secure access to web applications.

- **Risk-based authentication**. The ability to consider multiple factors, including device fingerprint, user behavior history, use location, etc., to determine the risk of allowing access for that user.

- **Fine-grained authorization**. The ability to provide very granular, flexible and externalized access control for applications.

- **Mobile/social authentication and authorization**. The ability to easily leverage established authentication and authorization mechanism for native mobile apps.

- **Identity federation**. The ability to extend authentication and single sign-on services across domain boundaries.

- **Enterprise SSO**. The ability to provide single sign-on services for all enterprise application types, including Web, thick client or legacy “green screen” applications.

Office of the Information and Privacy Commissioner, Ontario, Canada
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: 416-326-3333
Fax: 416-325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

Oracle
2355 East Camelback Road
Suite 950
Phoenix, AZ 85016
Phone: +1.602.333.9000
Fax: +1.602.333.9001

Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

September 2013

Information and Privacy Commissioner, Ontario, Canada

ORACLE