# Elevating the Discussion on Security Management

## The Data Centric Paradigm

Tyrone Grandison[*], Michael Bilger[#], Luke O'Connor[-], Marcel Graf[+], Morton Swimmer[+], Matthias Schunter[+], Andreas Wespi[+], Nev Zunic[#]

[*]IBM Almaden Research Center
650 Harry Road, San Jose, California.

[#]IBM Security & Privacy Services
2070 Route 52, Hopewell Junction, New York, , USA

[-]Zurich Financial Services
Mythenquai 2, P.O. Box 8022, Zürich, Switzerland

[+]IBM Zurich Labs
Säumerstrasse 4, Rüschlikon, Switzerland

*Abstract* — **Corporate decision makers have normally been disconnected from the details of the security management infrastructures of their organizations. The management of security resources has traditionally been the domain of a small group of skilled and technically savvy professionals, who report to the executive team. As threats become more prevalent, attackers get smarter and the infrastructure required to secure corporate assets become more complex, the communication gap between the decision makers and the implementers has widened. The risk of misinterpretation of corporate strategy into technical safe controls also increases with the above-mentioned trends.**

**In this paper, we articulate a paradigm for managing enterprise security called the Data Centric Security Model (DCSM), which puts IT policy making in the hands of the corporate executives, so that security decisions can be directly executed without the diluting effect of interpretation at different levels of the infrastructure and with the benefit of seeing direct correlation between business objective and security mechanism. Our articulation of the DCSM vision is a starting point for discussion and provides a rich platform for research into Business-Driven Security Management.**

***Keywords: Data security, Management decision-making, Resource Management, Security***

## I. INTRODUCTION

In a world where security and privacy breaches are increasing daily and new attacks become more damaging and harder to detect [1-3], the value of security controls becomes obvious, at least at a cerebral level. Enterprises are cognizant of the fact that business threats, such as network outages, production system compromise and the exposure of customer data, may not only lead to the interruption of business services but may also damage business reputation; especially if breaches are publicized. Despite this realization, companies still do not have convincing business metrics for evaluating a security strategy's effectiveness. Security spending is viewed as pure cost without a tangible business benefit; therefore it is to be minimized similar to other pure costs, such as insurance and raw material purchases. Consequently, a security conundrum arises: "security cannot be ignored" and at the same time "security must be cheap".

Security-conscious enterprises understand that managing Information Technology (IT) Security Risk is the critical element of their business resilience strategy. Lack of proper IT security controls places the entire enterprise at great risk. In the current business landscape, IT security mechanisms are not (directly or indirectly) correlated to business objectives. This lack of a direct link makes it is difficult to determine the right level of IT security to be employed by an organization and near impossible to justify investment levels in IT security controls.

In parallel to this phenomenon, it can be observed that business and technology factors are making traditional paradigms of computer security obsolete:

- Integration or federation opens enterprises to their partners and to attacks and fraud originating from their networks.
- Resource sharing, componentization and virtualization reduce barriers that once protected applications from each other.
- Provisioning engines and centralized directories (e.g. for identity, policy) become prime targets for hackers and single points of failure.
- Openness makes it easier for hackers to connect to and plug into widely deployed IT systems.
- Autonomic systems are allowing the automatic adjustment of bandwidth, computing resources and security defenses, which allow faster (and easier) propagation of security threats.
- Speed and adaptiveness (i.e. flexibility in addressing dynamic issues and implementing standard, pre-defined solutions without human intervention, etc.) amplify security problems.
- Business process transformation and outsourcing increase dependencies on third parties.

With such a complex array of factors and possible threats, an enterprise's main challenge is to implement the correct level of security that addresses the appropriate threats. The prioritization of their most pressing concerns is ultimately driven by business requirements, i.e. for each business asset, the appropriate level of protection is

implemented, which results in controls that are cost efficient and effective without being overkill.

This paper introduces the Data Centric Security Model (DCSM), which leverages the business value of data to determine and implement the appropriate level of overall IT security. In section II, we examine the perspective of a C-level executive (i.e. CEO, CIO, CTO, etc.) and highlight the tasks important to him in the security management process. Section III presents the conceptual details of DCSM, while section IV describes how DCSM can be deployed. The DCSM workflow is presented in section V and a staggered approach to achieving DCSM is presented in Section VI. Related work is presented in Section VII and we conclude in Section VIII.

## II. Life From The Eyes Of a C-Level Executive

Top-level executives worry about the long term prosperity of a company. As such, their primary responsibility is to ensure that there is a corporate vision and a business strategy that brings that vision into reality.

A business strategy is a plan for a company to obtain and sustain a competitive advantage. Business strategy objectives, which provide a context in which to measure and evaluate the strategy, typically address the following dimensions:

- Maximizing shareholder value.
- Retaining and attracting clients.
- Reducing the costs of business processes.
- Maintaining and improving market competitiveness.
- Maintaining business continuity and resilience.
- Achieving and maintaining regulatory compliance.
- Managing and enhancing marketplace reputation.
- Establishing new investments.
- Identifying and exploiting new business opportunities.

Information is vital to these strategic objectives. IT and security technologies, such as intrusion detection systems, extrusion detection systems, antivirus software, firewalls, data policy enforcement tools, audit tools and virtual private networks (VPNs), are critical to the efficient protection of systems that implement these objectives. But neither IT nor security are strategic objectives on their own. For business strategists (and in fact, most people), these technologies are merely components of a complex IT infrastructure designed to support the reliability and integrity of the core business. Looking beyond the details of technologies and practices, we observe that IT security is a large contributor to the business notions of trust establishment and risk mitigation, which impact most of the business objectives previously enumerated.

An executive's first security priority is to protect critical data, core processes and the trust that other enterprises, customers and stakeholders place in the enterprise. Clients and companies are more inclined to establish business relationships with a company they trust. These business alliances hinge on subjective evaluation. A company, particularly one that promotes itself as a brand, will be very concerned about maintaining its reputation as a trusted business partner. With respect to IT, trust manifests itself mainly in the way data is created, collected, stored, processed and distributed. Clients view companies as the custodians of their data, and expect trustworthy treatment of their data. Companies that outsource processes expect the same privileged treatment from the outsourcing service provider.

For clients, privacy is a paramount trust issue [4]. Clients need to be reassured that their data is protected from release or modification and is used only for intended business purposes [5, 6]. Recently, several high-profile disclosures of client data [1], through poorly protected databases accessible via the Internet, have caused a significant loss of reputation for the companies involved. The companies themselves are concerned with the integrity of their business processes and the data that supports these processes. In particular, if a business process involves interactions with a business partner, then additional care must be taken to ensure trust in the process as a whole.

The dependencies between security and business objectives manifest themselves in the execution and support of business processes. The specification, measurement and optimization of these dependencies, through a language that makes business value evident, are still difficult issues to get a handle on. Risk analysis, and in particular methodologies for operational risk management [7], provides a bridge between security technologies and their impact on business processes in terms of expected losses due to threat realization. Many companies are now adopting enterprise-wide risk management strategies in response to regulatory and compliance requirements, particularly the Sarbanes-Oxley (SOX) legislation [8]. Control Objectives for Information and related Technology (CobiT) [9] is one of the few well-developed methodologies for supporting such a strategy. However, current techniques depend heavily on the deterrent factor of audit-centric control mechanisms for ensuring compliance. In a majority of cases, irreparable damage to a firm's reputation and profitability may have already occurred before these controls have detected the security breach. Thus, these current set of control objectives need to be augmented with proactive methodologies that can immediately address security problems as they occur.

### A. *Proactive Executive Steps*

As a first step to bridging the gap between security and business objectives, the key corporate assets must be identified and their associated risks examined.

#### *1) Protecting Key Information Assets*

At the most basic level, today's enterprises are driven by their information assets, which are the most critical (and most valuable) business artifacts in the organization's possession. The reason is that:

- Information represents the know-how of an enterprise.
- Critical business processes operate on information.
- Trusted relationships are maintained by exchanging (possibly sensitive) information.

As a consequence, if the confidentiality, integrity and availability of the information are not guaranteed, the business will cease to exist.

However, all information was not created equal. From a business point of view, the level of security protection applied must be based on the business value of the information that is being protected. Since data is the core asset that must be protected by IT security controls, the business value of data must drive the mechanisms to be implemented, which is the central thought behind the DCSM.

To identify the business value of particular types of information, an enterprise can analyze the business value of the information, the business processes that operate on it, and the business relationships that it supports. This is a complex task that must be tailored for each enterprise; as financial companies will value their clients' investment information more than their employees' data. This is an area where research is needed and the community can make significant contributions. Currently, these valuations are made by service consultants with intimate and extensive knowledge of the enterprise. Once the value of the data has been determined, security control requirements can be defined and justified from a business perspective, based on the risk exposures.

*2) Risk Mitigation using Data Centric Security*

Managing the overall IT risk that an enterprise faces is another important business objective of IT. Enterprises are willing to bear a well-defined risk of a particular severity. Nevertheless, they want to ensure that they can afford the cost of exposures, i.e. damage to assets and brand, and that major incidents are unlikely and do not threaten the enterprise as a whole. One of risk management's important aspects is to implement an adequate level of baseline protection to ensure infrastructure availability.

Security management methodologies, such as ISO 17799 [10], are applicable to some of the previously enumerated business objectives, but there are no common metrics for comparing security methodologies with business objectives. This is not surprising, given that industries such as banking and insurance have developed over several hundred years, while computing is less than 50 years old and commercial IT security is much younger. ISO 17799 presents a methodology for providing and managing security services, as opposed to furnishing security professionals with a means to communicate security business value to their stakeholders. ISO 17799 can be viewed as a segmented island in IT management, which needs to evolve to become more integrated with business processes and strategy.

Unfortunately, IT security risk methodologies are immature [11, 12] and do not appear to be converging toward the analytical and predictive power of more established models, like credit risk models. Security risk practitioners are quick to point out that their task is severely handicapped by a lack of accurate, long-term security data, as compared with the voluminous data available for financial risk models. While this is true, there are no credible security risk models available that could process long-term security data, even if such data were available. The main issue seems to be that security professionals are not well versed in risk techniques that are quantitative and predictive.

The DCSM leverages these two steps that are performed by the executives. Let's examine the model itself and discuss how these tasks are incorporated.

## III. THE DATA CENTRIC SECURITY MODEL (DCSM)

DCSM allows organizations to overcome the disconnect between IT security technology and the objectives of business strategy. We propose to link security services directly to business processes by relating security services directly to the data they implicitly protect; a relationship that is often obscured by the presentation of security as an end in itself.

### *A. DCSM Core Principles*

The focus in the DCSM is on deriving the right security level, based on a business analysis of the data being handled. This data classification then drives the properties and access control policies governing the use of data by applications that implement business processes. Security services and their underlying mechanisms can be abstracted into interfaces that directly support data management policies. The DCSM does not require major changes to security services, but instead takes existing functionality, then casts and integrates that functionality in terms that can be directly understood by people who define and manage business processes. In this manner, security can be seen as directly supporting business processes and, in turn, business objectives.

As previously discussed, traditional risk management methodologies or other informal linkages between security and business processes have not proven to be sufficient. Thus, our approach of creating a direct dependency between the DCSM and business processes established, via the data acted on by processes. This is the primary contribution of this paper.

We emphasize that the DCSM approach does not create this link based on data, but brings to the fore the security methodology data components that are all too often obscured by security technicalities and terminology. All security technologies seek to protect data, and all security functions and protocols target appropriate data use.

The DCSM is mainly a re-statement; in terms of the data control capabilities supported by security services of current security models that focus on protection

mechanisms and management. Typically, these data control capabilities are not emphasized, but it is exactly this aspect of security services that will provide the linkage to business processes. More importantly, the DCSM does not depend explicitly on specific security products or technologies and is independent of the underlying security infrastructure. DCSM implies no modifications to the way policies will be enforced on the underlying IT system. It merely provides a means of specifying and mapping business requirements to tangible security controls.

The first consideration of a DCSM is to determine a set of guidelines for enterprise-wide data handling, based on business policies. The next consideration is to determine which security services are required to support these guidelines. We structure these guidelines into two parts. The first part classifies business data. A class can be based on the owner and on given security requirements, e.g.:

- Where did the data originate?
- Who owns the data?
- Who controls the data?
- Who or what holds the data?
- What type of data is it?

For each class, the business-oriented security requirements are defined that describe how a certain class of data shall be handled and protected. Example policy decisions that define how data are handled include:

- Who or what can use the data?
  - For what purpose?
  - Can it be shared?
  - Under what conditions?
- Where will the data be kept?
- How long do we keep the data?
- Does it need to be safeguarded?
  - At rest?
  - When backed up?
  - During use?
- How can the data be disclosed?
  - What subset can be disclosed?
  - What protection must be implemented?
  - Does the data need to be distorted or watermarked?

Each of these data issues has direct business significance; on protecting intellectual and business knowledge, maintaining the integrity of business processes, or adhering to and complying with jurisdictional regulations. The dependence between such guidelines and security services is also evident, i.e. the confirmation of data origin and ownership will rely on authentication and provenance services; data modification will rely on authorization, curation, auditing and access control services; data safeguarding will rely on confidentiality, privacy and disclosure control services; data storage will rely on integrity and reliability services. The mechanisms supporting these security services may be complex and are part of the IT infrastructure services, but these details are hidden in the DCSM.

In the security arena, emphasis is shifting from network-based to host-based defenses. If we extend this layered defense approach further, beyond host-based security to the data that is protected on those hosts, we arrive at the DCSM. To keep these multiple defense layers manageable, DCSM defines an integrated requirements and policy approach. Figure 1 illustrates this central tenet in the DCSM, where data is placed at the center of all activities and artifacts.

From the business side, the first objective in creating a DCSM is to identify the owner of the data, whether it's an individual, a customer, or a line of business. Requirements are gathered from both business and legislation governing usage and handling of specific types of data. These requirements will influence the policies that are defined and applied to the data. Data is classified using business terminology while access control policies are defined using organizational roles. Let's examine this model more closely.

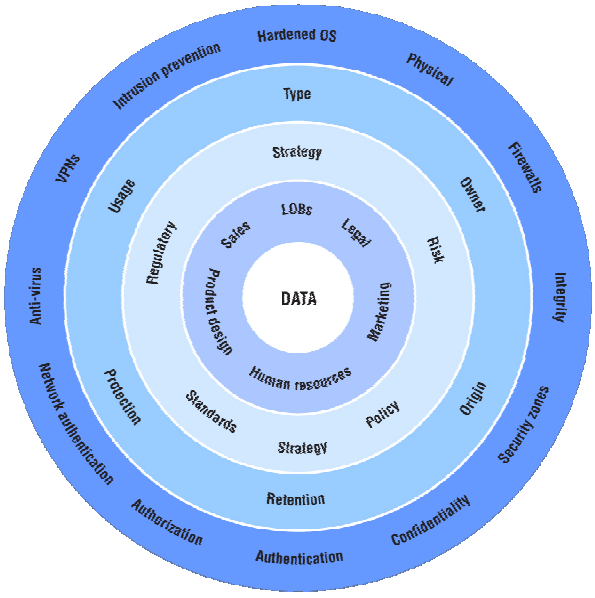


Figure 1. Data Centric Security Model

## B. *Components of the DCSM*

The main two components of the Data Centric Security Model are the policy and data pillars (Figure 2).

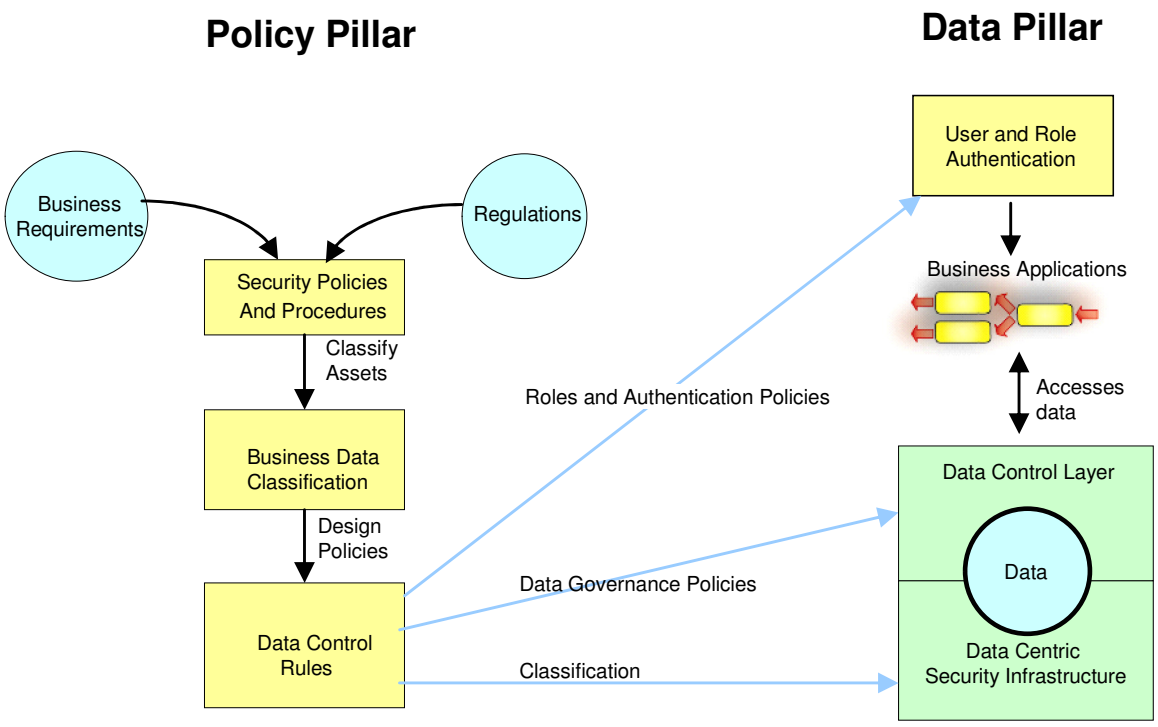


Figure 2. The components of the DCSM

The policy pillar starts by summarizing the business requirements and regulations that will be addressed by the security architecture. . Given that one C-level executive is normally tasked with IT infrastructure, we assume that this executive will gather the business requirements from all the stakeholders, resolve any conflicts between the multiple divisions and create the cohesive, consistent set of business requirements that affect the company's computing platform. For purposes of simplicity, we also assume that the executive is provided with a GUI that enables him to input the requirements and transform them to rules, which is a well-studied area of requirements engineering [13, 14].

Both requirements and regulations are unified into a description of the desired security policies and procedures for different data classes. The corporate and regulatory policies express data handling policies in terms of requirements, both internal and external to the enterprise, which, for example, may dictate obligations for data owners and custodians or may state data retention periods. The next step is to use the security and business requirements to define an overall business data classification (BDC), which represents the labels or attributes of data that are used to determine the data classes. Data will also be classified by criteria such as ownership, origin time and location. The data will have well-defined owners, typically expressed in terms of a business purpose or business line function. The goal is to identify the overall data governance that needs to be implemented. The data classification and the policy rules are encoded into data control rules (DCRs). These DCRs represent the unified data handling policies expressed in terms of BDC. They are used to establish appropriate access policies and practices to support corporate data handling policies.

The data pillar of DCSM rests on a security infrastructure that provides basic security functions, such as perimeter defense, protection of data at rest, or encapsulation of data during transmission.

Access to the data and permissible actions on the data are controlled by the data control layer (DCL). The DCL is designed to implement the (abstract) policies expressed in the DCRs and relies upon security and privacy services in the IT infrastructure. Its fine-grained controls can implement a wide range of DCRs. The DCL obtains the access context (such as authenticated users) and uses this context to decide whether the data can be accessed. The IT infrastructure is configured to support the security policies that have been derived from the DCRs. Business applications access the data through the DCL, which uses the data governance policies specified in the DCRs.

On top of the data pillar is a role-based authentication component that identifies users and assigns roles to the users based on authentication policies provided by the policy pillar. To enable protection with only minimal changes to the applications, we leverage an application abstraction model that maps terminology between application-specific contexts to the corporate data governance rules. This enables the DCL to understand application context without requiring that this context is adapted to the security policies.

The DCSM provides layers of protection that are consistent with corporate or organizational policy and regulations; as corporate standards are used to restrict (or allow) data access to users. The sensitivity of the data will

dictate the appropriate protection measures at every phase of a data request. The infrastructure's services are utilized to protect critical data, and the corporate risk acceptance plan will determine the appropriate use of technical safeguards at the infrastructure and application layers.

## IV. Deployment of the DCSM

Figure 3 shows an example of a logical deployment of the DCSM. The security infrastructure provides services to the DCL that are defined in terms of the data control policies. Here, a policy statement, such as data of type X that must be securely transported, would be translated into a request from the DCL to the secure transport service of the security infrastructure. This service in turn may rely on a protocol such as SSL, which itself makes uses of certificate-based authentication, but these details will be hidden from the DCL. If the data requester is a mobile employee, then the safe transport requirement may, for example, be satisfied by using a tunneled VPN connection, again a detail hidden from the DCL.

Thus, the DCSM depends on: an enterprise-wide BDC scheme, consistent deployment of the DCL at the point of access to all data and adherence to data classification during capture, transmission, and storage. The last requirement implies that data labels are persistent and must reside with the data that is labeled. Let's drill deeper into the details of the DCSM workflow.

## V. The DCSM Workflow

We previously hinted at the activity workflow and technical concerns involved in using the DCSM. In this section, we present these topics more explicitly, in order to highlight the issues and possible research areas.

### A. *Design of Classification and Policy*

The first phase is an initial execution of the policy pillar. This execution includes identification of the critical data types that exist in an enterprise, as well as the business and regulatory requirements that apply to the data. Based on these consolidated security requirements, specific security requirements for each data category can be derived. To implement the required protection, the security staff then designs critical-data system policies that meet the security requirements put forward for each of the categories. This flow is depicted in Figure 4. This process could be helped by investigations into the space of business-driven policy specifications for security enforcement, business policy refinement, design tools for data classification and conflict resolution for business and legislation requirements.

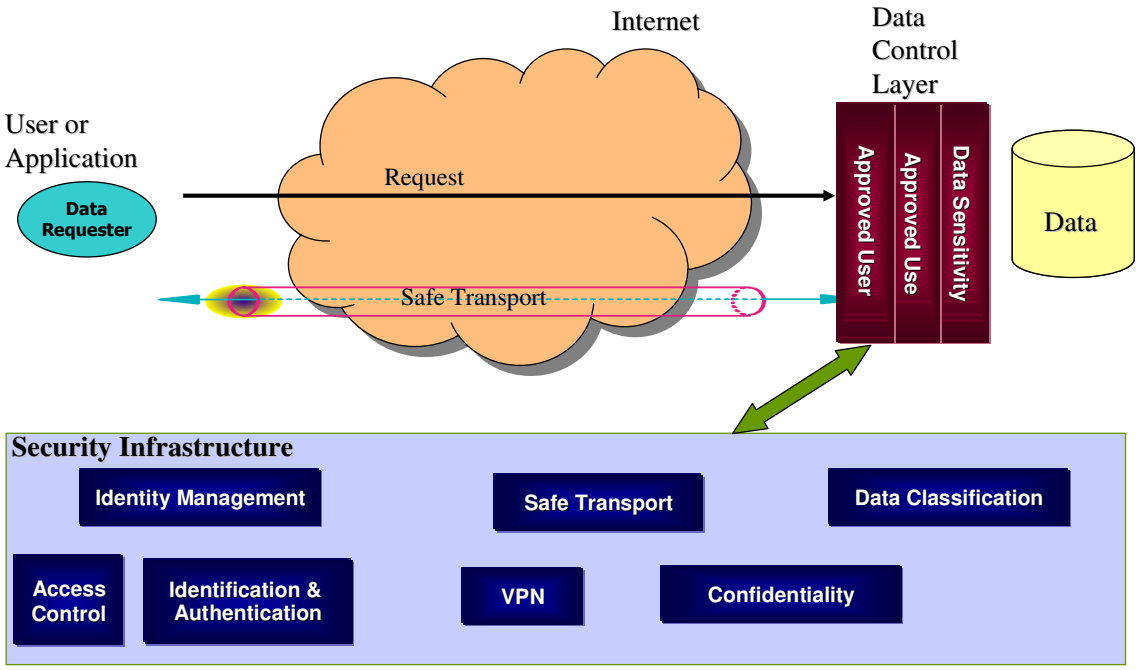


Figure 3. A logical deployment of the DCSM.

### B. *Migration: Classifying Business Data*

Data handled by an enterprise must be associated with classifications. Classification can be done on several levels. The most coarse-grained approach is to label security zones with the data classifications that they are allowed to process. The next-finer-grained approach is to label systems and channels with the data classifications that they are permitted to process. The next refinement is to label databases and channels in detail. This approach requires that, for example, the classification of the columns of a database is determined and stored. The most fine-grained approach is to label individual instances, for example, to identify which files are classified confidential.

DCSM is based on the ability to classify data according to a common schema. Recall that the original goal of the DCSM was to provide a direct linkage between security services and the data of business processes. Clearly then the data classification of the DCSM must be defined in terms of business data, as opposed to any existing security classification schemes, because in the DSCM security

requirements are subordinate to the data's business value. Therefore, sensitivity labels commonly associated with mandatory access control (MAC) are unsuitable to form the basis of a data-classification schema. In military security models based on MAC policies, information assurance policies dictate data-handling practices independent of the use of data in various processes [15]. In a commercial setting, this approach is inappropriate.

A data model based on the operation of business processes can be linked downward in the enterprise architecture to security services and linked upward to the business modeling and architecture layers. Such a business data-classification schema can provide closer affinity to corporate security policies for data classification in agreement with business processes and may lead to increased security awareness for employees who can directly understand the business purpose of data they are handling. Also, such a data model is expected to ease the definition of inter-enterprise agreements for data exchange. Research contributions on automated business data classification would be invaluable in this step.

### *C. Authentication and Authorization: Role-Based Data-Access Control*

Authentication, authorization and disclosure control are at the heart of the DCSM and several components are needed. An authorization component asks the user for authentication and issues corresponding user credentials. A monitor component observes accesses to critical data and requests authorization to perform the desired operations. A role-based data-access component decides whether a policy allows or denies a certain operation on a given data category.

This policy enforcement engine is a core component of a DCSM design. It obtains the roles of the user accessing a data category, the business context of such a business process and the operations to be performed on the data. The rules-based engine then returns a decision: whether the access is allowed, denied or filtered. The engine can also determine if transformations should be performed on the data before release [16]. Depending on the criticality of the data, authorization may either prevent unauthorized access or generate corresponding non-compliance events. Low cost and low impact authorization and enforcement technology would benefit both the security and DCSM worlds.

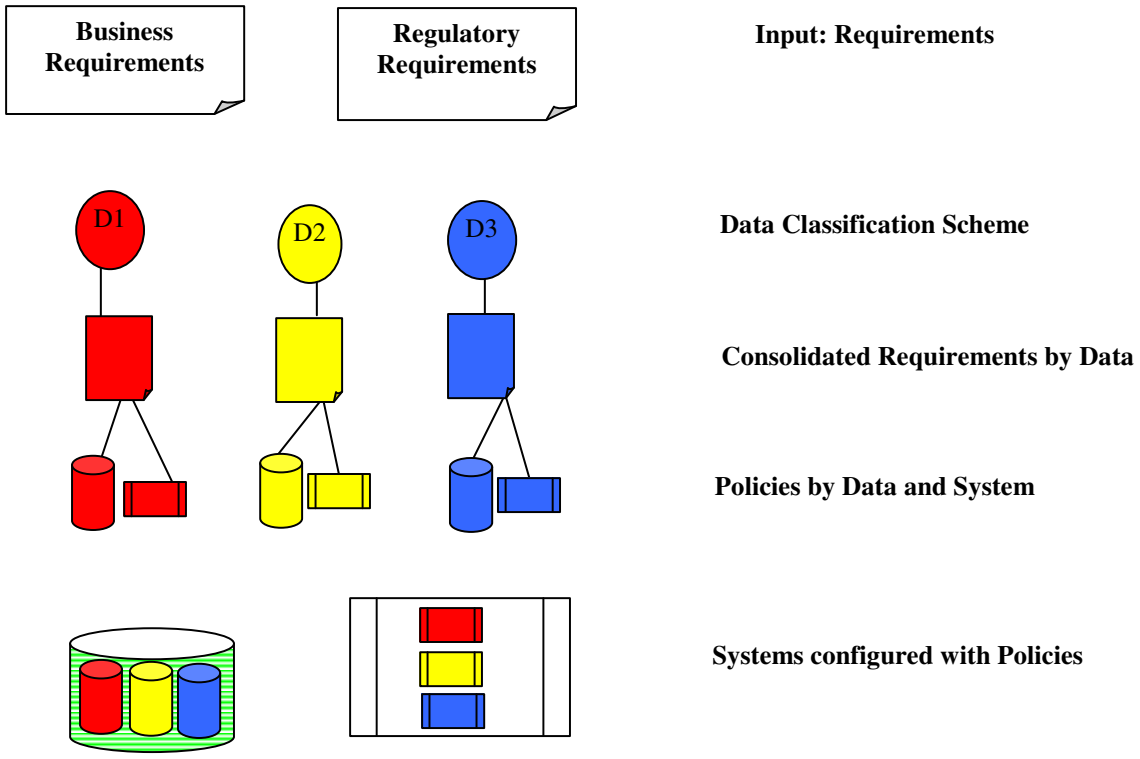


Figure 4. Security Analysis and Policy Design

### D. Policy Management

Data centric security is based on a new approach to policy management, in which policy design is federated between multiple authorities inside an enterprise. It is essential for compliance that the overall enterprise enforces certain baseline policies. The security team and the business process owners define a baseline policy for business classification along with mandatory rules for handling the data categories. Each business owner can further refine the policies and make them more granular, if necessary. Additional policies can also be added by the business process owners. The policy management system then ensures that these local refinements do not violate the mandatory enterprise-wide policy. This is another fertile area for the research community to participate in.

### E. Inter-Enterprise Transactions

Enterprises are increasingly moving toward value networks in which groups of equal partners form short-term coalitions similar to virtual enterprises. Business trends suggest that this model, in which each enterprise concentrates on its core competency while most transactions cross organizational boundaries, is expected to be the rule rather than the exception.

For such inter-enterprise transactions, data must be seamlessly protected, no matter where it is currently located. From a data centric approach, this requires that labels be transmitted, and that the corresponding security requirements are globally enforced. In enabling such a unified enforcement in a heterogeneous environment, it is essential to note that each partner will use different policy implementations. The only common requirement is that the enterprises follow a data centric approach and that these policy implementations satisfy the given requirement. Examination of distributed data enforcement technology, sticky policy paradigms and schema & data integration would provide great mechanisms that can be leveraged by the DCSM.

### F. Foundation: Infrastructure Security

Data centric security requires a secure infrastructure, or at least an infrastructure with the adequate level of security services. If servers and systems are affected by worms and viruses, the ability to enforce a given policy is limited. As for all other secure systems, the higher the security requirements on data protection, the higher the infrastructure security requirements. As a result, any implementation of data centric security will require a basic level of system security. This means perimeter defense, patch management, identity management, virus protection, intrusion detection and disclosure control.

By labeling data, data centric security enables enterprises to proactively assess and manage their information assets. An enterprise will know the business value of the data handled by the different systems on different networks and will be able to split its infrastructure into different zones that correspond to the business value of the data that is handled within each zone. For zones that handle only low-value data, infrastructure protection can be reduced to the bare minimum, allowing investments to be focused on zones handling higher-value data. As corporations vary in size and capability, it may be necessary to provide varying levels of DCSM enablement. We present our thoughts on this in the next section.

## VI. Staggered DCSM Incorporation

The cost of deploying a system that embodies the DCSM philosophy may be prohibitive depending on the particulars of a company. To align with the business objectives, it may be necessary to stage DCSM deployment according to the current business risk and the business requirements for different parts of an enterprise. To guide this staged deployment, we outline the basic maturity levels for data centric security. An enterprise can then choose at which level of maturity to implement DCSM and in which parts of its operations. The maturity levels can be classified according to the matrix shown in Table 1.

TABLE I. Maturity matrix for data centric security

| **Adoption levels** | **Basic** | **Intmd.** | **Advanced** | **Full** |
|---|---|---|---|---|
| Security Infrastructure | Yes | Yes | Yes | Yes |
| Business data classification | | Yes | Yes | Yes |
| Role definitions | | Yes | Yes | Yes |
| Policies by classification | | Yes | Yes | Yes |
| Data is labeled | | | Yes | Yes |
| Data flow analysis | | | Yes | Yes |
| Automated policy provisioning | | | | Yes |

### A. Basic Maturity: The Status Quo

Basic maturity is the prevalent state in many enterprises. The security functionality is not driven by the business requirements on the data handled by the IT systems. Instead, general IT security requirements have been defined that implement a protection level designed to protect critical information assets. As a consequence, many assets are over-protected, while the most critical information assets are usually not sufficiently protected.

### B. Intermediate Maturity: Using Data Centric Security for Designing Security Policies

For adoption of data centric security, IT security investments must be driven by the protection needs derived from business requirements on the data. The first step is for business and IT to agree on which data categories will be protected. In addition, business must define the protection requirements for each data category, including requirements for baseline protection. Given these business objectives, basic data centric security is implemented by determining the most critical data that is handled by a system. Then the security controls that correspond to the required protection level are implemented. For intermediate maturity, the runtime classification is not reflected in the system. As a consequence, policies will be designed per system and need to sufficiently protect all data handled by a system.

### C. Advanced Maturity: Labeled Data

The next maturity level in adopting data centric security is to enable runtime labeling of channels and data while enabling automated policy selection. For example, an application server on this maturity level will be able to apply different access

control rule sets for different types of data. The labels are used to select the appropriate policy to protect given data.

### D. Full Maturity: Data Centric Security

A full implementation of data centric security comprises the mechanisms of the previous two maturity levels. Policies are designed from a data-classification perspective and data is labeled in the runtime system. Full data centric security implements automated policy management. The goal is for systems to adapt their security controls to the data they need to handle.

A system will have multiple policies that are applied depending on the classification of the data that is handled. These policies will be designed independently and then provisioned for the different system types. The core security requirement is that each data classification's corresponding policies satisfy the security requirements for that classification. There are two main approaches to guarantee compliance with this security requirement.

The bottom-up approach collects all corresponding policies and audits them for their compliance with the overall security requirements. A top-down approach formalizes the security requirements into baseline policy rules. These rules are then translated into system policies that can be automatically provisioned to the individual systems handling the data.

## VII. Related Work

The DCSM is related to work in the Security Policy, Database Management, Risk Management and Data Classification research areas. As stated previously, the Data Centric Security Model is technology agnostic and can leverage current and emerging techniques in the Security Policy (e.g. Discretionary Access Control [16], Mandatory Access Control [16], Role-based Security Specification [17], etc.), Data Management (e.g. Hippocratic Databases [6], etc.), Risk Management (e.g. decision theory algorithms) and Data Classification (e.g. Kazeon's classification technology, eClassifier technology, etc.) spaces.

In [19], da Costa et. al. provide insight to technical staff on implementing and controlling enterprise security governance policies, which should be considered a complementary educational process for DCSM deployment.

Aib et. al. [20] propose a policy-based management framework geared towards IT professionals that realigns IT network infrastructure with a company's business objectives. Their emphasis is on network reconfiguration and optimization in the context of service providers and service level agreements. The business stakeholders of the system do not seem to enter the discussion.

In their paper entitled "Enforcing Business Rules and Information Security Policies through Compliance Audits" [21], Yip et. al. propose a XML-based specification that allows the definition of multiple legislation and provides the first step in the provision of compliance auditing support. However, it does not have support for specification of real business objectives and their connections to real security mechanisms.

## VIII. Conclusion

There are dependencies between IT security services and business objectives, but there is no unifying principle to express and evaluate these dependencies. Security technologies are too arcane to be of central interest to strategists, and the importance of IT security may simply be relegated to the IT infrastructure. Risk methodologies are not advanced enough to provide a convincing bridge between security technologies or services and business processes. The DCSM provides a first step in addressing these problems.

The purpose of the Data Centric Security Model (DCSM) is to directly align business strategy and IT security through the common thread of data. This paper represents an initial conversation in allowing business people to more tangibly see that there is an intrinsic Return on Investment (ROI) for security technology purchases.

We presented a new approach to security, whose primary goal of is to drive security controls from a business requirements perspective. This goal is achieved by separating policy and classification from data protection. For each data class, appropriate controls can be defined that reflect the business requirements that have been identified by an enterprise. DCSM complements the current set of audit-based controls and requires no change to the current IT infrastructure of a company. DCSM purports analysis of the data assets of a firm and the translation of business requirements into deployable IT rules.

Overall, data centric security enables cost-efficient protection of information assets. Unlike today's approach of providing unified protection to all assets, data centric security uses business requirements to design and implement a specific level of protection for each asset class that an enterprise holds.

The ability to update security policies in operational systems provides the flexibility needed to adapt to changing regulatory and business requirements. This easy and intuitive way to maintain overall security policies is designed to be cost effective, while allowing businesses to flexibly address changing security requirements in a dynamic business environment.

Given the fact that each industry and, possibly, each firm in an industry will require a customized deployment of DCSM, the vision and generic model presented must be tailored for each engagement. However, the higher level concepts discussed here always apply.

The intention of this paper is to spark discussion on models for enabling Business-Driven Security Management and on the technology and research contributions that need to be made to make this a robust reality.

## References

[1] Privacy Rights Clearinghouse, "A Chronology of Data Breaches", http://www.privacyrights.org/ar/ChronDataBreaches.htm

[2] Privacy Rights Clearinghouse, "How Many Identity Theft Victims Are There? What is the Impact? Summary of Survey Findings", http://www.privacyrights.org/ar/idtheftsurveys.htm

[3] SANS, "The Ten Most Important Security Trends of the Coming Year", http://www.sans.org/resources/10_security_trends.pdf?ref=2411

[4] J. Rachels, “Why Privacy is Important”, Philosophy and Public Affairs, Vol. 4, No. 4 (Summer 1975), pp. 323-333.

[5] K. Kailing, A. Löser and V.Markl, "Challenges and Trends in Information Management", Datenbank-Spektrum, Volume 6, Number 19, 2006, pp. 15-22.

[6] R. Agrawal, J. Kiernan, R. Srikant and Y. Xu. "Hippocratic Databases". Proc. of the 28th Int'l Conf. on Very Large Databases (VLDB 2002), Hong Kong, China, August 2002.

[7] J. L. King, “Operational risk : measurement and modeling”, Publisher: New York : Wiley, 2001.

[8] Securities and Exchange Commission, “Sarbanes Oxley SEC Rules”, http://www.sarbanes-oxley.com/section.php?level=1&pub_id=SEC-Rules.

[9] Information Systems Audit and Control Association (ISACA), “CobiT4.0: the newest evolution of control objectives for information and related technology, the world’s leading IT Control and Governance Framework”, http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/COBIT40-Brochure.pdf

[10] International Organization for Standardization, “The ISO 17799 Directory”, http://www.iso-17799.com/

[11] H. Cavusoglu, B. Mishra and S. Raghunathan, "A model for evaluating IT security investments", Communications of the ACM, Vol 47, Issue 7, 2004, Pages 87-92.

[12] J. F. Broder, “Risk Analysis and the Security Survey”, Publisher: Boston : Butterworth, 2000.

[13] R. Young, "Putting Requirements Theory into Practice at Northrop Grumman," , Proceedings of the 14th IEEE International Requirements Engineering Conference (RE'06), 2006.

[14] C. B. Haley, J. D. Moffett, R. Laney and B. Nuseibeh, “A framework for security requirements engineering”, Proceedings of the 2006 international workshop on Software engineering for secure systems. Pg: 35 - 42. 2006

[15] T. Ager, C. Johnson and J. Kiernan, “Policy-Based Management and Sharing of Sensitive Information among Government Agencies”, Proceedings of the 25th IEEE Military Communications Conference, Washington DC, USA, October 2006.

[16] K. Lefevre, R. Agrawal, V. Ercegovac, R. Ramakrishnan, Y. Xu and D. DeWitt. "Limiting Disclosure in Hippocratic Databases". Proc. of the 30th Int'l Conf. on Very Large Databases (VLDB 2004), Toronto, Canada, August 2004.

[17] R. Sandhu and P. Samarati, “Access Control: Principles and Practice”, IEEE Communications Magazine, vol. 32(9), pp. 40-48. 1994.

[18] M. D. Abrams, “Renewed Understanding of Access Control Policies”, Proceedings of the 16th National Computer Security Conference, Baltimore, Maryland, U.S.A., pp. 87-96, 20-23 September 1993.

[19] L. daCosta, G. Alves and A. Almeida, "Enterprise Security Governance - A practical guide to implement and Control ISG (Information Security Governance)", Proceedings of the 1st IEEE/IFIP International Workshop on Business-Driven IT Management, Vancouver, Canada. April 7, 2006.

[20] I. Aib, M. Salle, C. Bartolini, A. Boulmakoul, R. Boutaba and G. Pujolle, "Business Aware Policy Based Management, Proceedings of the 1st IEEE/IFIP International Workshop on Business-Driven IT Management, Vancouver, Canada. April 7, 2006.

[21] F. Yip, P. Ray and N. Paramesh, "Enforcing Business Rules and Information Security Policies through Compliance Audits", Proceedings of the 1st IEEE/IFIP International Workshop on Business-Driven IT Management, Vancouver, Canada. April 7, 2006.