Ontology of Information Security in Enterprises

Stephen Schiavone[1], Lalit Garg[2] and Kelly Summers[3]
[1]University of Liverpool, Fountain Hills, Arizona, USA
[2]University of Liverpool, University of Malta, Malta
[3]Medicis Pharmaceutical Corp, Scottsdale, Arizona, USA
steve.schiavone@my.ohecampus.com
lalit.garg@my.ohecampus.com
krsummers@sbcglobal.net

Abstract: Today's global free-market enterprise is reliant on the interconnectedness of social, economic and political ecosystems. Enterprises no longer maintain a simple unary relationship between its customers and consumers. Enterprises have become an integral part of a complex relationship within the new socio- and techno- economic paradigm. The cornerstone of this new model is the Internet formed from a collection of eclectic commodity-based and inconsistently constructed technologies that, at an aggregate level, do not lend themselves to provide a secure and trustworthy channel to conduct or transact business. Enterprises have struggled to implement an appropriate and continuous level of protection in part by underestimating the effect of organizational complexity and not adopting a holistic (systems thinking) approach to the problem of enterprise security. This research paper examines key issues that undermine the ability of enterprises to formulate effective and viable security models and proposes an alternative framework that forms the basis and foundation to engineering more reliable fail-safe and fail–secure models. The proposed solution considers the creation of an enterprise-specific ontology that describes the enterprise as a complex system. A security framework is developed that recognizes the organization as a set of business capabilities that have measureable strategic outcomes against which business decisions regarding security are made. The proposed model advocates symmetry between security prevention, prediction and fail-safe concepts. To ensure the appropriate use of security, a business value model is defined that is a function of financial, operational and security-based quality assurance measures. The concept of value chain is used to describe the relationship between an organization's strategy and its resources responsible for the execution of its operating plan. Validation of the 'Enterprise Ontology' and 'Information Security Capability-Driven Framework' is obtained from the creation of a business strategy to 'business capability value map' and quantification of key business and security metrics. A set of ontology-based competency questions allows the business to understand and make informed and prudent decisions regarding how and where security should be applied to ensure a favourable outcome for the enterprise. Analysis of the results of this study demonstrates the usefulness of the model in guiding the organization to assess current security risks and make informed and business-directed security decisions. The result is a deployment strategy that balances the scarce resources of the enterprise whilst maintaining strategic alignment. Further opportunities exist to improve the creation and quality of enterprise ontology including development of a more rigorous and systematic approach to modelling the enterprise's current state and future state scenarios using the business capability framework. Semantically driven conceptual models of the enterprise may also be expressed within key security technologies and systems that support the organization by forming a collection of ontology-aware technologies that respond and react collectively to attacks in a fail-secure configuration.

Keywords: ontology, fail-secure, fail –safe, reliability engineering, frameworks, business capability, IT security

1. Introduction

Technology has, at an unprecedented level facilitated the rapid propagation of age-old criminal practices of espionage, sabotage, criminal syndicates, extortion, theft, subversion and persecution at a global level. In a 2012 study of data breach incidents between medium and large International companies, the following findings were presented (Verizon RISK Team, 2012). [1] The motivations behind cyber-crimes are financial (96%). [2] The majority of successful attacks (96%) are the result of an organizations' poor understanding of security and poor deployment of security measures. [3] Whilst compliance to specific security standards, best practices or adherence to specific control frameworks such as CobiT (COBIT, 2006) were made, poor use of such models created a false sense of security and drove enterprise complacency. [4] The study reported that 75% of organizations were compromised in minutes from attack to data exfiltration regardless of the size and maturity of organization or the amount of money invested in information security. [5] Detection of a security breach took months (54% of cases). [6] Containment and restoration of services took weeks (38% of cases). The ease at which opportunistic attacks were successful in achieving their goals suggests in this study that organizations are ill prepared to deal with cyber-threats.

Cyber-threats have become sophisticated and technically well engineered. Attacks used in industrial espionage in the form of Advanced Persistent Threats (APT) demonstrate that attackers are well resourced, determined and meticulous in their approach. The use of malware is advanced, detection difficult and persistent even upon detection, containment and removal. In a report by NASA (Martin, 2012), it was revealed that there were 47 APT attacks, 13% were successful in compromising systems and stealing user credentials enabling attackers to gain access to NASA computing resources. In 2011 a top security vendor RSA was compromised using APT and zero-day vulnerabilities techniques (Munro, 2011). RSA's two-factor technology was successfully exfiltrated compromising the integrity of millions of devices used across all industries including the military. In 2011, an APT attack (Night Dragon) was successfully used for the purpose of Industrial espionage against Oil, Energy and Petrochemical companies (McAfee, 2011). In 2009 W32.Stuxnet infected over a 100,000 hosts across several industrial countries (Falliere, Murchu & Chien, 2011). W32.Stuxnet targeted the control systems of power plants and gas pipelines by modifying assembler code on specific programmable logic controllers. The malware used demonstrated complex behavior characteristics by introducing a root kit to hide the malware binaries, and used advance techniques for code injection.

Kshetri (2010) reported that the global economic impact of cyber-crime in 2009 was up to US $1 trillion. Between 2005 and 2007 the average loss from fraud per company increased from US $1.7 million to US $2.4 million. In the United States, (one of the largest economies in the world) cyber-crime cost the country approximately US $400 Billion which is approximately 4% of its Gross Domestic Product. In the UK, cyber-crime accounted in 2008 for GB £6 Billion.

The speed of attack, compromise, data exfiltration, sabotage, and delays in detection and recovery indicates that organizations are ill prepared to deal with cyber-threats despite advances in security-based technologies, evolution of security related frameworks and industry-specified best practices. Cyber-attacks are growing and continuing to have significant economic, social and political impact. Countermeasures have proved difficult to apply in part caused by confusion surrounding the nature of cyber-crime within the enterprise (Kshetri, 2010).

The purpose of this research paper is to propose a holistic approach to information security expressed in the form of its ontology and management framework centered on business capabilities derived from an enterprise's strategic goals and objectives and the use of specific enterprise domain resources viz. people, processes and technology (Burton, 2010). The framework proposed is referred to as Capability-Driven Information Security Model (CDISM). The idea behind unification is twofold:

- The enterprise is viewed as a complex and dynamic system (Sterman, 2000) that modifies its behavior by changing its internal structure in response to internal and external pressures that are typically commercial or financial in origin (Sackmann, 2008). Security must be continuous and adapt to changing conditions.
- Cyber-attacks are considered instances of complex systems (McAfee, 2011) insofar as they are purposeful, adapt to their environment (through causal feedback loops), replicate and modify their surroundings (Falliere, Murchu and Chien, 2011). To address such behaviour requires a more holistic rather than selective (atomic based) security model.

In the context of complex systems, a successful risk management strategy must consider what is known including mitigation strategies and unknown (improbable) cyber-threats. This is expressed in terms of security prevention, prediction and fail-secure models respectively (Benzel et al, 2005 and Avižienis et al, 2004). The former is managed by understanding business impact of a known threat through probabilistic cause and effect modeling. The latter is managed by understanding emergent effects created by indeterminate cascading failure effects (Rebovich, 2011). The focus of security becomes the protection of the interdependent resources responsible for the successful execution of an enterprise's strategy rather than the protection of an enterprise's general assets that are supported by contemporary models (Fenz and Neubauer, 2009). The CDISM framework becomes an integrated rather than fragmented approach to the security of the enterprise, incorporating in one single consideration the interdependent resources of people, process and technology. A systems thinking approach examines the issues of cyber-attacks in a novel way (Meadows, 2008) whereby successful cyber-attacks are achieved not because of their ingenuity or technical sophistication, but because the enterprise unwittingly sets up the necessary conditions for such attacks to be successful. If an enterprise considers cyber-attacks linear, the risk management and countermeasures activities are based upon (linear) cause-and-effect principles applied to events known (*a priori*), limiting the effectiveness of any security model applied (Simmonds et al., 2006). As new cyber-attacks are deployed, the enterprise assesses its likelihood of

occurrence and probabilistic business impact forcing the enterprise to be forever in a reactive mode driven by cause-and-effect mechanics. A security model that reacts to an ever-growing number of cyber-threats will typically strain and exhaust the resources of an enterprise. It is unrealistic for an enterprise to secure itself against all known cyber-threats. A more effective and efficient approach is to selectively focus on security issues that is facilitated by what the enterprise considers worthy of safeguarding dictated by strategic imperatives, engineered and delivered through business capabilities. Such capabilities are serviced and supported by a collection of interrelated and interdependent resources (entities). Such an approach shifts the conversation of security from external considerations (reactive mode) to internal analysis and deliberations (proactive mode), enabling the enterprise to thoughtfully allocate and engineer resources in accordance with business needs, risk and benefits. Such an approach evaluates the resilience and reliability of the enterprise structure (resources) without necessarily understanding the essence of the attack. The approach facilitates a proactive method based essentially on a balance between preventative, predictive and fail-safe security models.

CDISM framework is based upon the principles of unification, complex systems behavior, failure analysis, reliability and resilience (dependability) and alignment to business strategic imperatives.
The research goals are summarized as follows:

- To define and develop an enterprise-wide information security model that leverages ontological concepts and principles to express the complex and dynamic nature contained within an enterprise.
- To develop an operational description of the notion of security, detailing metrics and measures necessary to facilitate enterprise-wide resource allocation management to aid the execution of business strategy.
- To define a conceptual framework that provides consistency, focus and alignment between an enterprise's mission statement and business strategy, security position (condition or status), and enterprise domain resources responsible for the execution of its strategy.

2. Design approach

The ability of an enterprise to devise a cohesive and coherent security model is dependent on understanding several important aspects of information security as applied to complex enterprises. In particular, it requires:

- Ontology for the enterprise, a clear and precise description of the nature and context of an organization including its ecosystem of element interactions.
- Understand the properties of improbable threat events and its impact to the underlying structure and performance of the enterprise i.e. its failure mode (Avižienis et al, 2004).
- Dependable security metrics and performance measures applied at the (holistic) enterprise level and (atomic) resource level.
- A conceptual framework (Clark, Guba and Smith, 1977) that defines an appropriate security model mapped against an explicit business strategy and enterprise capability.
- Understand the internal structure and emergent behavior of the enterprise during failed-state scenarios.

3. Ontology

Expression of the complex nature of the domain enterprise is achieved through the creation of ontology repository using Protégé (Protégé, 2012). Development of enterprise ontology benefits business decision-makers in that the complex relationship is expressed in business terms rather than information technology and security terms. The importance of ontology is to remove confusion and ambiguity when discussing key concepts within the world of security. Lambrix, (2010) maintains that ontology is useful in that it facilitates:

- Communication between people and organizations
- Defines a common vocabulary that facilitates the sharing of knowledge within an organization
- The creation of an authoritative source of security information.

Noy & McGuiness (2012) includes the following characteristics of ontology:

- Maintains separation of domain and operational knowledge

- Provides the basis of domain-based knowledge enquiry
- Making obvious domain assumptions simplifying the enhancement or modification of acquired knowledge

The ontology for a Capability-Driven Information Security Model is represented in the following model (Figure 1). Key considerations for its description are:

- The domain in focus extends beyond the four walls of an enterprise and considers the ecosystem in which its existence is defined viz. extended enterprise
- Expands beyond the risk model of asset, vulnerability, threat and countermeasure and includes business and technical capabilities, complexity and failure mode scenarios
- Defines new vocabulary for security, value, enterprise and service
- Creation of useful security driven metrics

From Figure 1, an enterprise [2] with input from investors and shareholders [1], defines its mission i.e. describes the enterprise's market uniqueness or distinctiveness, from which a strategy, and execution approach with key performance measures are created (2 ▸ 3). enterprise objectives [3] are derived from the enterprise mission statement [3] that in turn defines the commensurate business and technical capability plan (3 ▸ 7). Business capabilities define an enterprise's competitive advantage in the market place. Not all capabilities are new, modifications can also be made to existing capabilities due to internal and external pressures for example continuous improvement efforts driven by efficiency and effectiveness goals (2 ▸ 7) or an enterprise's relationship (4 ▸ 7) with external entities [4] caused by changes to commercial agreements, or mergers and acquisitions. Other influences are derived from governance [5], regulatory, legal, industry specific and fiscal policies (6 ▸ 7). Influences and changes to the nature and characteristics of business and technical capabilities are driven from the enterprise's Reference Architectures (9 ▸ 7) that describes key standards and consistencies in the way domain resources are created, aligned, utilized, and maintained. This is considered the critical success factors in a capability-oriented framework. Reference Architectures are reflective of influences that occur to changes in standards, designs, configurations and operationalization parameters. Its influence spans the entire enterprise from business services, business processes to the underlying application and technical infrastructure. An example of such influences may stem from known vulnerabilities [13], threats [11] and countermeasures [12] that are by no means restricted to just the technical infrastructure (13 ▸ 7, 11 ▸ 7 and 12 ▸ 7). Vulnerabilities and countermeasures may leverage and use ontologies [14] external to the enterprise (14 ▸ 13 and 14 ▸ 12). Such concepts reinforce the belief that an enterprise is fluid and constantly changes. In this regard security must respond accordingly [6] and in a timely manner.

A business capability is comprised of the following entities: business services, business processes, business activities, tasks, people, organization units and application and technical services. Process steps are orchestrated and coordinated through automated or manual workflows. Business processes may share the same resources creating the notion of shared services (meta-resources) and dependencies between processes and workflows reinforcing the idea of complexity within the enterprise and risk is seen as an emergent property. In this regard vulnerability, threats and countermeasure focus not on individual components but holistically against a business capability [7]. The domain-oriented model provides the following advantages:

- Enables the enterprise to focus (contextually) on those resources that define the business capability value stream that require protection rather than focus upon discrete well-known points of vulnerability and threats. By focusing on the business capability security is focused across large areas of the (Extended) enterprise
- Describes in business terms the relationship and complexity between items within the enterprise and extended enterprise
- Provides an understanding of an organization's current protection strength and competence in quantitative and qualitative terms
- Provides a metric-based approach to understanding current organization proficiencies against the requirements imposed by a new capability
- Allows the organization to assess cost and effort required to support a business capability information model through the information life cycle. This is driven in part by designing, constructing, configuring and

operationalizing a set of domain resources that meet the Security Quality Assurance goals (for example dependability or reliability metrics)

Within the Capability-Driven domain, known vulnerability [13], threats [11] and counter-measures [12] define and drive elements of dependable and resilient resources (12 ▸ 9 and 13 ▸ 9) that based on failure mode analysis manifests into a resilient and reliable set of enterprise business capabilities (9 ▸ 7). Due to the concept of the extended enterprise [4], security will consider and protect business processes and interactions that traverse the four wall of the enterprise (11 ▸ 4 and 13 ▸ 4) for example, trading in confidential information.

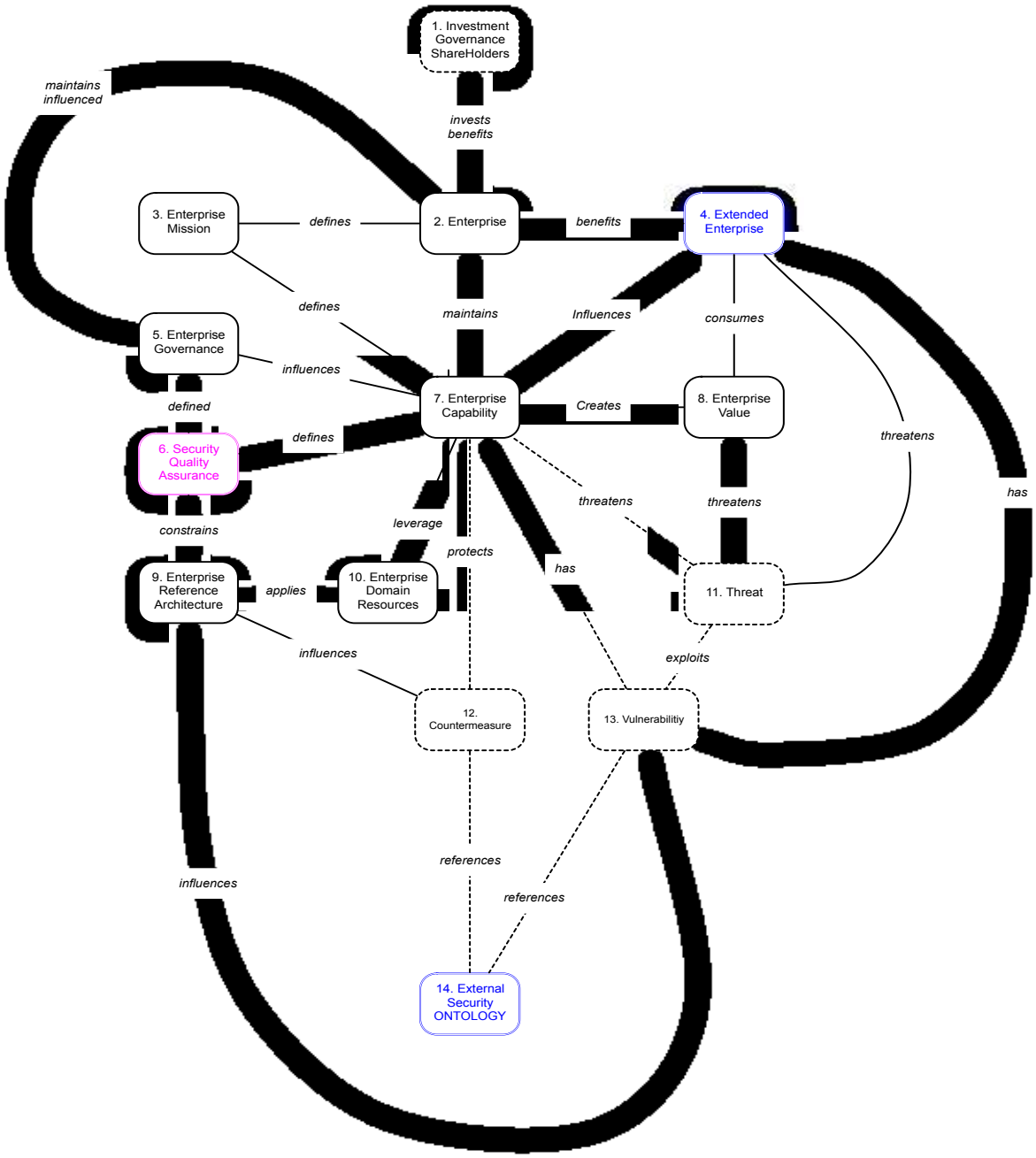

Figure 1: Capability Focused Information Security Model

Business capabilities [7] create business value [8] i.e. (7 ▸ 8) that is consumed by external entities (8 ▸ 4). Value may be services or products an enterprise offers. Business value may also directly benefit people within the enterprise (e.g. culture, and ethics). The enterprise [2] and Shareholders [1] benefits from value chain transactions (4 ▸ 2) in terms of revenue, profit, market share gain, and earnings per share (2 ▸ 1).

Security quality assurance [6] is viewed as a set of design and operationalization controls (measures and key performance indicators) used to ensure that the designed operational run state that each business capability has achieves its intended design goals and objectives thereby maximizing business value. Such controls also protect the enterprise against degraded run states produced intentionally or unintentionally by (importantly) unknown threats. Security resiliency of a business capability may be seen in terms of the number of failures taken to move a capability from a known good state into a degraded state or inoperative state. Security Quality Assurance [6] influences how business capability [7] solutions are engineered for dependability i.e. fail safe model (6 ▸ 9) and is influenced by policies derived from compliance policies (5 ▸ 6).

The mechanism used to define, create and deploy such resiliency is found in the CDISM Framework.

To provide focus and scope to the development of ontology for a Capability-Driven Information Security Model a set of (competency) questions are produced. Such questions serve to validate and verify the described ontology.

- What is the objective of a business capability for the enterprise as defined by its business mission, vision, and strategy statements. Such understanding provides the required context and focus for a security-based quality assurance model
- Define the relationship between the enterprise, extended enterprise, business capability and business value. Such understanding describes in business terms the degree of enterprise complexity in question and the areas of security focus
- Define the security quality assurance requirements for a defined business capability (expressed in quantitative and qualitative terms). This establishes the design parameters that a business capability will operate and is expressed in business-speak
- Identify the enterprise domain resources required to define and describe a business capability. This describes the relationships and dependencies between the enterprise resources
- Define the business value proposition of a business capability. This establishes the alignment of a business capability with the enterprise mission statement and provide an area of focus
- Define the current security quality assurance baseline for the enterprise domain resource of business services,application services and infrastructure services. This describes in business speak the dependability index, investment value and effectiveness measures for the enterprise as a criterion
- Define the security quality assurance requirements for a business capability. This is expressed in measures of “Investment” and “Dependability”. This describes the effort and investment required to support a business capability. The business value of such an enquiry drives a balanced business decision in terms of cost, risk and benefit.

The developed enterprise ontology is based upon the knowledge of an existing commercially viable organization, Medicis (Medicis Pharmaceutical Corporation, 2012) leveraging existing business strategies and resources and those derived from other sources to create a more elaborate model (Renkema, 2000 and Weill and Broadbent, 1998). The domain of the enterprise is shown in Figure 2. This view represents the key relationships between major classes and sub-classes within the ontology. The enterprise specific ontology is based on an approach defined by Noy and McGuinness (2002) and is comprised of eight super class types: *Enterprise*, *Enterprise Capability*, *Enterprise Domain Resources*, *Extended Enterprise*, *Enterprise Governance*, *Enterprise Reference Architecture*, *Enterprise Mission*, and *Enterprise Value*. Descriptions of the most influential classes are discussed as follows:

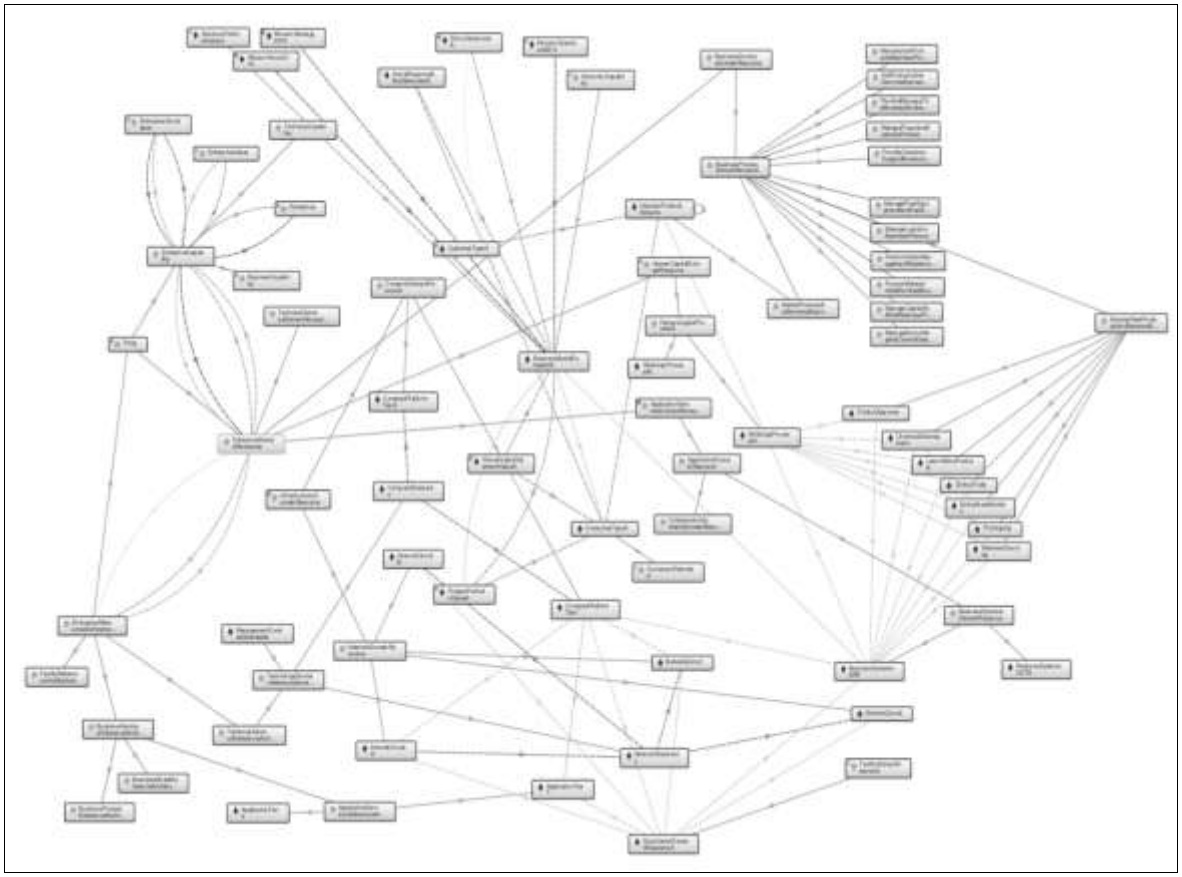

Figure 2: Enterprise domain

3.1 Enterprise

Defines the entity enterprise from which the *Mission Vision*, *Mission Strategy* and *Mission Objectives* class instances are expressed. The class instances describe the identity of the enterprise and its reason for existence (Guevara, 2011).

3.2 Enterprise capability

The class *Business Capability* contains the *business model* class instance that describes the goals and objectives of the example capability seen in quantitative and qualitative terms. The properties of the class *Business Capability* define the dependent *Domain Resources* required to deliver such a capability and define the business value proposition expressed in terms of Financial (Downes and Goodman, 2010), Operational (Smith, 2010) and security-specific Quality Assurance performance measures.

3.3 Enterprise domain resources

Enterprise Domain Resource is the most complex class, consisting of thirty-four sub-classes of which the topmost are: *Application Services*, *Business Services* including business process models (Deloitte, 2012), *Human Capital* and *Technical Services*. This class represents the enterprise resource classes required to support and execute a business capability (Barroero, Motta and Pignatelli, 2010).

3.4 Enterprise extended

This class is important in terms of enterprise security and defines the ecosystem within which the enterprise functions as a part of its business model. The underlying premise maintains that the security of the enterprise extends beyond its four walls.

3.5 Enterprise reference architecture

The idea behind the creation of sub-classes within this entity is to reduce the level of technical variability or heterogeneity within the complex system. This is accomplished through the use of established standard design patterns applied to each class of domain resource. This approach minimizes potential conflicts between the interdependent resources by moving the complex system from a state of potential chaos to relative stability. Within this domain class, the concept of reliability of systems through concepts of fail-safe models is used.

3.6 Enterprise value

The purpose of the class *Enterprise Capability* is to generate enterprise value in the form of the value sub-classes: *Product*, *Services*, *Shareholder*, *Social* and *Ethics* (Nightingale, 2005). The class *Enterprise Value* is aligned to *Enterprise Mission* and *Enterprise Capability*.

4. Results

Alignment of enterprise resources to business value is achieved by understanding the knowledge contained within enterprise ontology and defining the security quality assurance measures and leveraging the CDISM framework.

4.1 Ontology

This is achieved by interrogating the ontology repository in light of a set of pre-established competency questions (Noy and McGuinness, 2002), examples of which are shown in Table 1.

Table 1: Ontology competency questions

5. Competency Question	6. Rationale
Define the required Security Quality Assurance measures needed to support the enterprise's current Mission.	This establishes the design parameters that a Business Capability will function. This is usually expressed in business narrative (summarized in Table 2).
Define the current Enterprise Capability, i.e. its baseline (reference) model.	This describes in business terms the dependability index, investment value and effectiveness measures for the enterprise expressed in Financial, Operational and Security measures (summarized in Table 3).
What is the effort needed to meet the performance requirements of a newly defined Enterprise Business Capability.	This describes the resource targets and level of effort and investment required to support a Business Capability. The business value derived from such an enquiry drives a balanced business decision in terms of cost, risk and benefits (summarized in Table 3).

The results of such enquiries are partly summarized in Table 2. Important information contained in this table is expressed in both qualitative terms (columns A, B and C) and quantitative terms (columns D, E and F). The business capability identified in this research is called *Product Diversification Strategy* and is expressed within the ontology as a class type *BusinessModelDomesticA* (column G). The table describes a single business capability (A) that contains three classes of performance measures that are functions of *Enterprise Business Value* viz., Financial (D), Operational (E) and Security (F). The strategic value of the capability is defined in terms of revenue and profitability goals, market share and product performance goals (Smith, 2010) such as Product Profitability Index (PPI), Market Share Index (MSI) and Time to Market Index (TTMI). The resultant security (quality assurance) measures are an interpretation of the former two metrics expressed in terms of resource dependability, effectiveness, investment, information sensitivity and strategic value. This provides the enterprise with areas of focus, direction and location of security efforts.

Table 2: Business strategy mapping to business capability and performance measures

Business Capability [A]	Improve product innovation and delivery into new Markets maximizing revenue (product diversification).
Value Metrics and Measures [B]	Focus on speed to existing markets and new markets. Market share and revenue creation are primary drivers. Operating efficiency is important, as are CR, STR, and TTMI. Operations model is high available indicating high reliability and low failure impact.
Objectives (Intangible Goals) [C]	Improve R&D capability, increasing product innovation and prototyping. Improve logistics and supply chain i.e. maintains 24x7x365 operations. Operations model is high available indicating high reliability and low failure impact.
Required Financial Performance Measures [D]	CR = 2.0, Profitability = 10.4%, EPS = 10, Revenue = $25,000,000, STR = 0.9
Required Business Performance Measures [E]	MSI = 7%, NCI = 10%, NPI = 15%, OTI = 22%, PPI = 82%, SII = 60%, TTMI = 1.5
Systems Capability Performance Measures [F]	R_c = 0.995, E_c = {0.999, 0.9, 3000}, S_c = {0.4, 0.6, 0.8, 0.5}, I_c = $1,000,000, V_c = 20%
Assessment [G]	Product Diversification Strategy **(BusinessModelDomesticA)**

6.1 Security quality assurance (SecSTAT)

Security in this research is viewed as the ability of an enterprise to maintain operational and financial viability (Jallow et al, 2007) during normal operating state in a trustworthy manner and exhibits predictable behavior in the event of a partial or total failure i.e. its fail –secure characteristics engineered into the solution. To minimize catastrophic events, enterprise resources must isolate a failed state event (R_c) by minimizing emergent effects that arise within the system as the result of a breakdown or failure (Kristen et al, 2008). The class, *Enterprise Reference Architecture* becomes a critical success factor in the construction of fail-safe resources driven from the capabilities design requirements (Peterson, 2007). The cause of a failure may be the result of a cyber-attack (intentional) or error (unintentional fault).

Security is multidimensional and is a function of the following variables. Business capability's Strategic Value (V_c), is expressed as $\{0.25 \leq V_c < 0.20\}$ and is a measure defined as the percentage of revenue contribution against total income. Strategic value enables the business to understand the relative importance of one business capability over another and establishes the concept of importance and prioritization. Capability Dependability, (R_c) is expressed as $\{0.995 \leq R_c < 0.990\}$ and is the measure of trustworthiness of a resource. A value close to 1 assumes with high certainty that the resource will not fail or will fail in a predictable manner. Capability Effectiveness, (E_c) is expressed as $\{A_c, U_c, P_c\}$ and is the performance characteristics of any one resource. A_c is availability, U_c utilization level and P_c performance of a resource. Business Information Sensitivity Classification, (S_c) is expressed as $\{I_s, P_s, S_s, IP_s\}$ and is the type and class of business information that is created and used by the Business Capability. The expression highlights the level of importance and criticality of information that flows within and outside the enterprise. Investment (I_c), is expressed as $\{0.101 \leq I_c < 0.095\}$ and represents the run-maintain costs of the resources responsible for executing the business capability. This is calculated as a percentage of cost against revenue generated by a business capability. Preservation of the integrity and trustworthiness of a business capability is expressed as a relationship between Financial, Operational Measure, Security Quality Assurance Measure and Business Value. Their relationship is shown diagrammatically in Figure 3.

The relationship between business value and security quality assurance measures ensure that the focus and effort required to secure the enterprise is aligned to its strategic goals (Jallow et al, 2007). As a business model is defined and subsequently changes due to external market pressures or internal efficiency drivers, performance measures (operations and finance) will change forcing the business value proposition (associated to a business capability) to change. As security is a function of business value, particular aspects of the security model must change in response. The effect of the shift is the recalibration of the enterprise's core resource capabilities and triggers a reevaluation of effort and focus in the management of the security model. Table 3 details the enterprise's current resource-specific operational state and compares this to the required (desired) state that is created by either a new, enhanced or modified business capability.

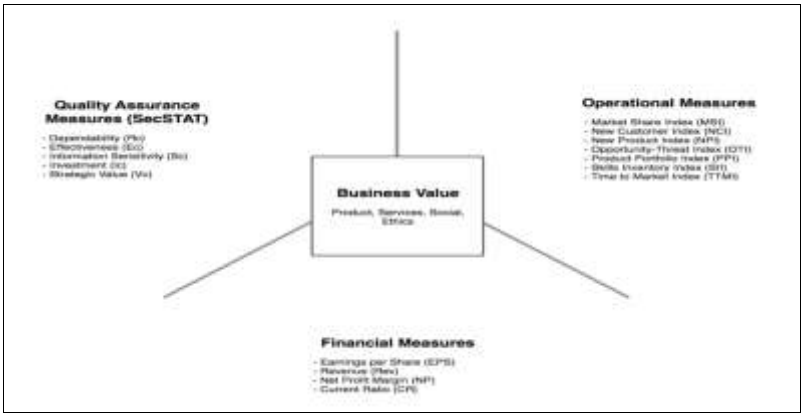

Figure 3: Business value model

Table 3: Current resource level capability compared to target capability

Object Type	7. Required Capability	8. Resource Dependency Dimension – Determined Current Capability			
Super Class	EnterpriseCapability	EnterpriseDomainResource	EnterpriseDomainResource	EnterpriseDomainResource	EnterpriseDomainResource
Class	BusinessCapability	ApplicationDomainResource	BusinessServicesDomainResource	TechnicalServicesDomainResource	TechnicalServicesDomainResource
Sub Class	DomesticCapability	BusinessSystemsDomainResource	DevelopNewProductsAndServicesBusinessProcess	InfrastructureDomainResource	InfrastructureDomainResource
Individual Class Instance	BusinessModelDomesticA	BusinessSystemsERP	ChemicalDevelopment ClinicalTrials	ComputePlatformTier1	NetworkZone1
Financial Measures	10.0	-	-	-	-
EPS	0.9	-	-	-	-
STR	25,000,000	-	-	-	-
Revenue	10.4	-	-	-	-
Net Profit	2.0	-	-	-	-
CR					
Operational Measures	7.0				
MSI	10.0	-	-	-	-
NCI	15.0	-	-	-	-
NPI	22.0	-	-	-	-
OTI	82.0	-	-	-	-
PPI	60.0	-	-	-	-
SII	1.5	-	-	-	-
TTMI		-	-	-	-
SecSTAT Measures	0.995				
R_c	{0.999,0.9,3000}	0.999	0.999	0.999	0.999
E_c	{0.4,0.6,0.8,0.5}	{0.990,0.4,3000}	{0.999,0,0}	{0.999,0,0}	{0.999,0,0}
S_c	1,000,000	{0.4,0.9,0.9,0.6}	{0.4,0.8,0.9,0.9}	{0.1,0.9,0.9,0.8}	{0.9,0.8,0.7,0.7}
I_c	20.0	120,000	0	10,000	10,000
V_c		-	-	-	-

Analysis of the Business Capability's required dependability (security) measure (R_c) is 0.995 and a capability's operational availability E_c {A_c} of 0.999. This suggests that the probability of a business disruption event of *P* A(0.005) and *P* B(0.001) is likely to occur over the life of the capability due to resource failure or unavailability of key resources. This is expressed by the equation *P*(A+B)=*P*(A)+*P*(B)-*P*(A)*P*(B) (O'Connor and Kleyner, 2012).

The loss of dependability and operational availability will impact the business value of the capability V_c ($25,000,000) resulting in a potential loss (in this example) of revenue circa $150,000. Emergent effects of the

failure are considered by examining the failure effects of the interdependent relationship between resources based on the ontology shown in Figure 4.

Information Security (S_c), expressed by {0.4, 0.6, 0.8, 0.5}, indicates that the information flow of the capability contains data that is high in private, sensitive and intellectual property (due to new product research and development). Loss of S_c can have larger organizational implications than simply a loss of revenue. Examination of the individual resource S_c parameters becomes an area of security focus. S_c is related to the dependability value of each resource. Loss of intellectual property can, in worst case, result in the loss of the business capability viz., V_c = zero (Ekelhart, Fenz and Neubauer, 2009).

Each resource's individual class instance contains the attributes associated with security assurance measures. This is influenced by the classes *Enterprise Governance* and *Enterprise Reference Architecture*. Based on its ontology, the cumulative values for R_c, E_c, S_c, and I_c are computed and compared to the needs of the business capability. Variances between actual state and desired state provide the organization with a means to measure the effort required and where to allocate scarce resources.

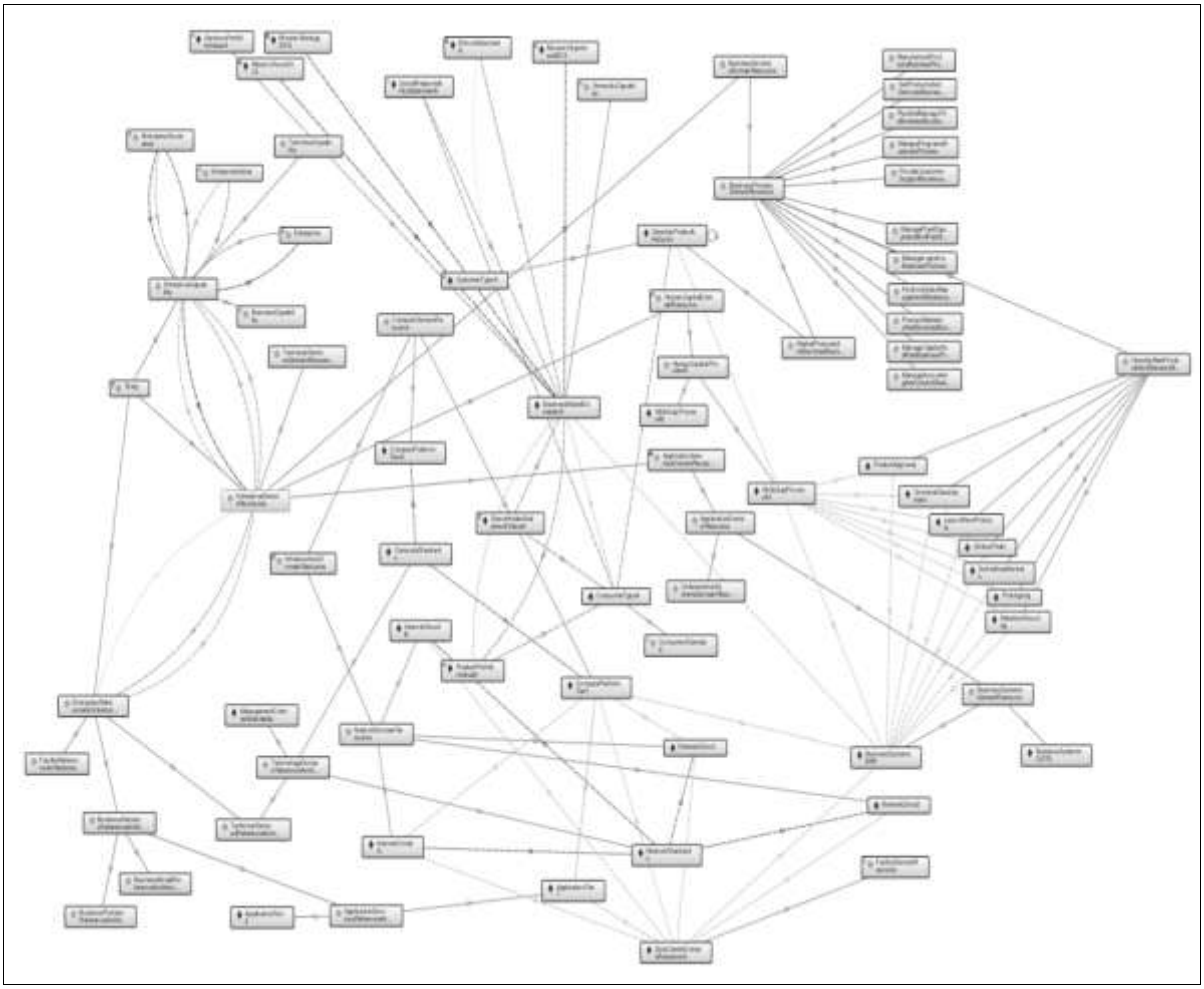

Figure 4: Ontology of enterprise domain resources

The ontology describes the complex nature of the concepts and relationships between the interdependent resources (Smith and Welty, 2001) that are required to successfully execute and meet the objectives set for the business capability called Product Diversification Strategy.

8.1 Information security conceptual framework

A business capability is seen as the proficiency or competency of the enterprise to deliver business value to its customers by leveraging interdependent domain resources spanning the entire organization (Kristen et al

2008). To ensure alignment between *Enterprise Strategy*, *Business Capability*, *Business Value* and related domain resources (internal and external), a framework is established. In the context of this research, a Business Capability Information Systems Model (CDISM) is developed (Figure 5) by binding principles of enterprise ontology, enterprise strategic planning, business planning and information technology and security principles. The components of the framework are Enterprise Capability Assessment, Business Capability to Strategy Alignment, Business Capability to Resource Mapping, Business Capability to Resource Alignment and Operational Run State. (Excluded from this study is the Operational Run State process that provides security actions through reinforcing and balancing causal feedback loops.) Each phase receives input from a number of internal and external sources, which may include ontology, enterprise strategy, business planning, governance and regulatory compliance directives and information technology engineering directives.

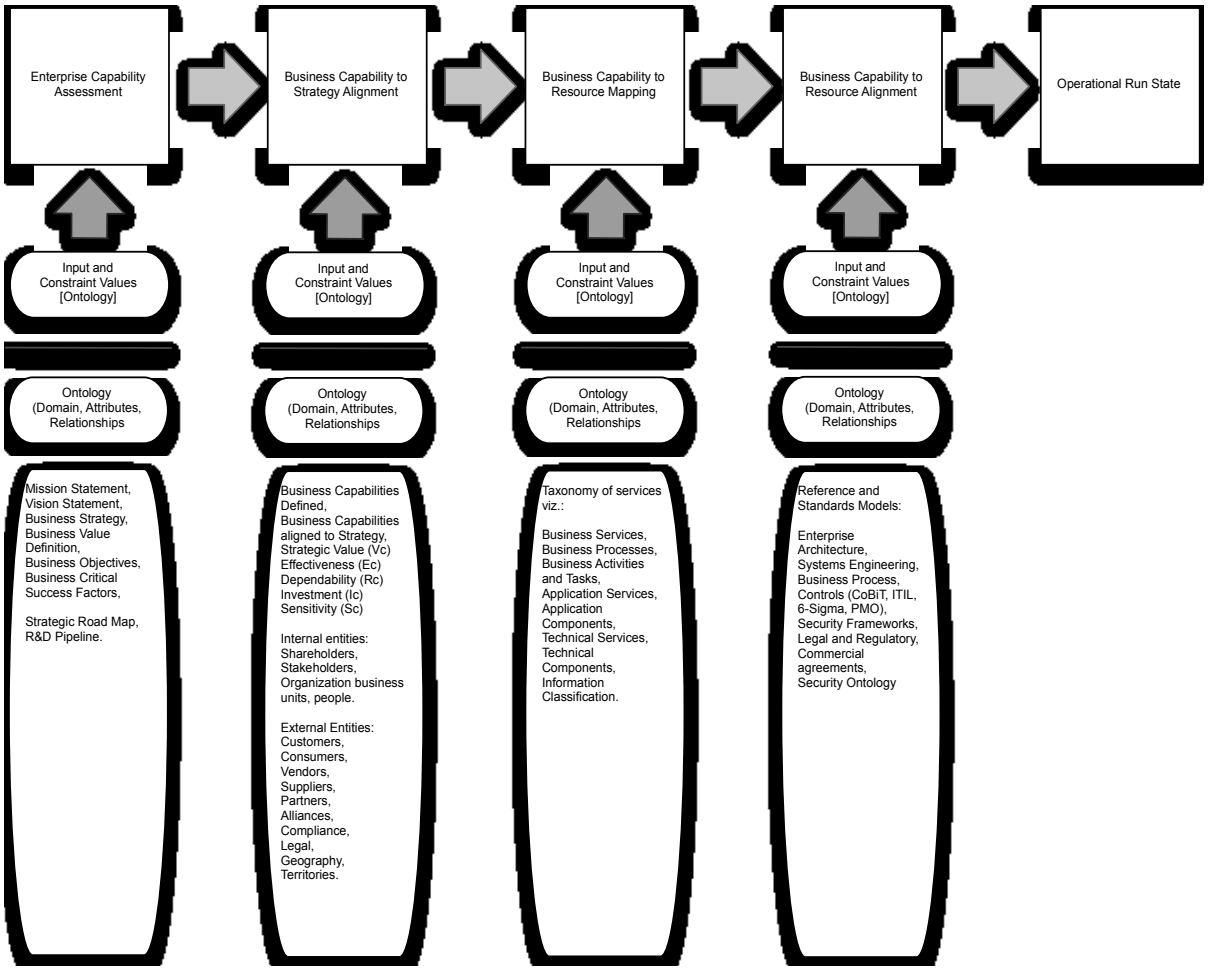

Figure 5: Capability-driven information security mode

Figure 6 provides a conceptual view of the relationship between *Enterprise Resources* sub-class *DomesticCapability* and sub-class *BusinessSystemsDomainResource* (Milanovic, Milic and Malek, 2008). A similar model (not shown) is developed to illustrate the relationship at the technical services level.

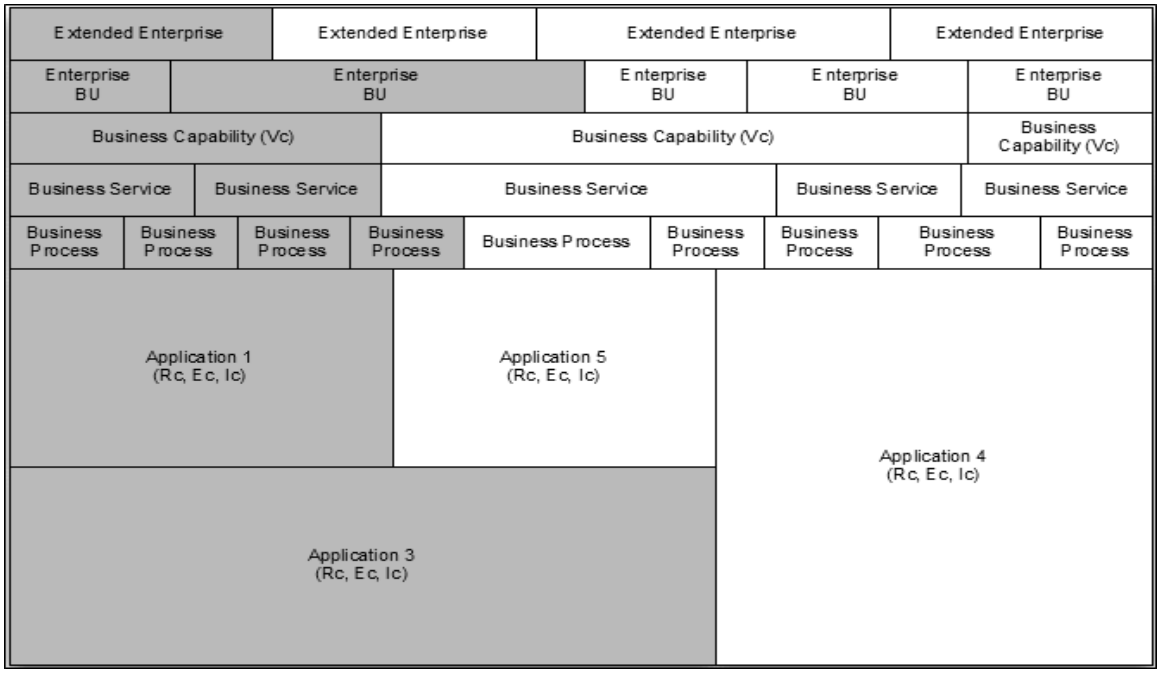

Figure 6: Enterprise resource reference model

Reliability of supporting technical resources configured in a fail-secure manner is engineered using the reliability modeling tool, BlockSim 8.0 (http://www.reliasoft, 2012). The resultant design is leveraged across business capabilities dependent upon that service. Figure 7 shows the relationship and dependability of the components within class *Enterprise Domain Resource*, subclass *Compute Platform Tier 1*.

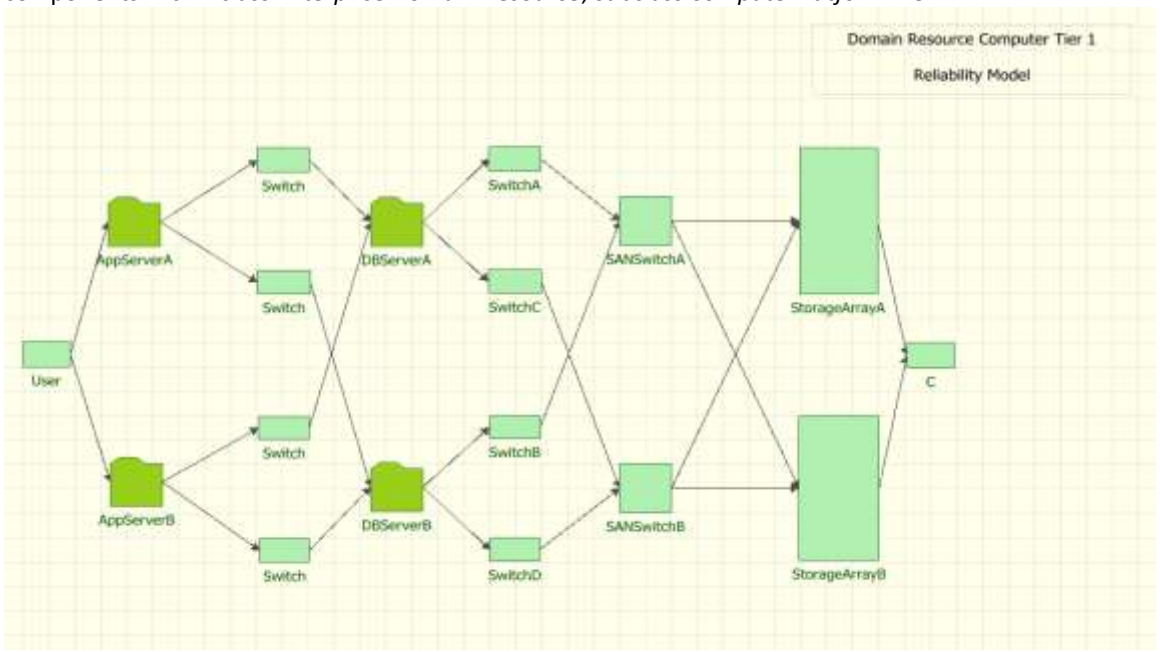

Figure 7: Domain Resource - Compute Platform Tier 1

Using what-if simulation models will identify where within the domain resource subclass improvements are to be made and importantly the cost associated with such improvements (figure 8). If a business capability identifies the need to support a higher level of reliability in this example R = 0.9900, a simulation is used to indicate where within the system such improvements are to be made and to what level of resiliency each component is adjusted for example the current value for Application Server A is R = 0.874388, to derive an overall system reliability of R = 0.9900, the reliability of the server needs to be set at R = 0.98622

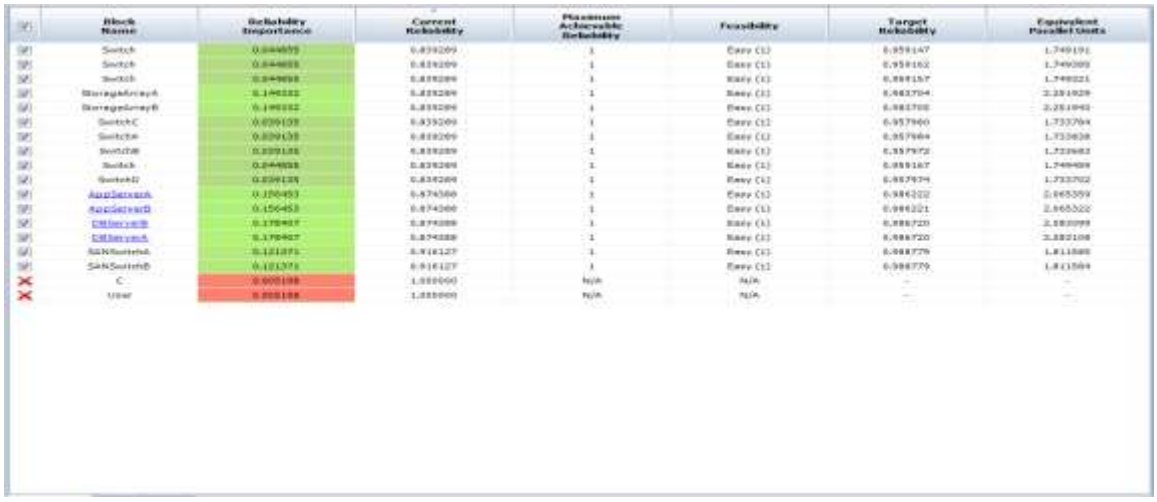

Figure 8: Target Reliability per Component - Compute Platform Tier 1

This approach drives several other measures viz. availability (within the Effectiveness metric), and effort expressed in terms of cost and time. An important cost driver in the Investment equation is the maintainability of the service. Here availability is defined as the effort that is required to restart a failed or degraded service. The following model figure 9 outlines the typical costs associated with maintenance and its impact to the availability and reliability of the Compute Platform Tier 1 (enhanced) service, viz. $40,307. This becomes an input into the Investment measure (Ic). Additionally, other costs come into play such as acquisition-deployment cost, payroll, and consultancy and contractor fees.

	A	B	C
9			
10	**System Overview**		
11	General		
12	Mean Availability (All Events):	0.999922	
13	Std Deviation (Mean Availability):	6.4E-005	
14	Mean Availability (w/o PM, OC & Inspection):	0.999922	
15	Point Availability (All Events) at 365:	1	
16	Reliability(365):	0.9916	
17	Expected Number of Failures:	0.0084	
18	Std Deviation (Number of Failures):	0.008798	
19	MTTFF (Day):	43282.87926	
20	System Uptime/Downtime		
21	Uptime (Day):	364.971647	
22	CM Downtime (Day):	0.028353	
23	Inspection Downtime (Day):	0	
24	PM Downtime (Day):	0	
25	OC Downtime (Day):	0	
26	Total Downtime (Day):	0.028353	
27	System Downing Events		
28	Number of Failures:	0.0084	
29	Number of CMs:	0.0084	
30	Number of Inspections:	0	
31	Number of PMs:	0	
32	Number of OCs:	0	
33	Number of OFF Events by Trigger:	0	
34	Total Events:	0.0084	
35	Costs		
36	Total Costs:	40307.54838	
37	Throughput		
38	Total Throughput:	8674.826304	
39			

Figure 9: Cost Associated to Maintain Targeted Reliability and Availability

Enquiry of enterprise ontology will determine for a particular capability the degree to which resources at the atomic level will meet the strategic objectives set at the enterprise Strategy level. Examination of the nature of the underlying structure and relationships will determine the degree to which certain resource attributes of Dependability (R_c), Effectiveness (E_c), Privacy (S_c), and investments (I_c) are aligned to the requirements of the enterprise. Examination of potential failures and cascading effects at the individual class instance provides the enterprise with the ability to determine the impact of failure and the level of investment required to meet its strategic objectives.

The process defined within the CDISM framework is repeatable throughout the business life cycle of the enterprise.

This research paper presents an alternative approach to dealing with the rise of cyber-threats made against enterprises. The uncomplicated world of cause and effect analysis and actions in response to threats and attacks are no longer sufficient and are in many instances outmoded as emerging cyber-threats have adopted the nature and characteristics of complex systems. Security frameworks must consider the complex nature of the enterprise and must understand and appreciate its internal structure and behavior in response to entity or resource failures. To enable the development of an alternative security model this paper identifies three main prerequisites. Firstly, there must be available an enterprise ontology - a universal model that is clear and precise and describes the complex structure explicitly. Secondly, security must be defined in terms that would allow an enterprise to understand clearly its meaning and apply it appropriately as it makes strategic, tactical and operational decisions. Finally, to ensure that the complex structure of an enterprise maintains alignment between interdependent resources and strategic imperatives, a framework is needed to leverage ideas of strategy and business value as it creates or modifies business capabilities. Alignment within the framework is achieved through business value that is a function of Financial, Operational and Security measures.

In this study, enterprise ontology was created to describe the complex structure of a real world enterprise (modified). Business value was defined in terms of a set of metrics that cascades directly from the organization's business strategy and expressed in a single business capability (Product Diversification Strategy). Ontology was used to understand the organization's current strategic competency and capacity at the resource level (individual class instance level). Such knowledge was used to evaluate the requirements of a future capability against current capabilities. A Capability-Driven Information Security Model (CDISM) was utilized to derive in a systematic manner the areas of focus within the enterprise and level of effort required to protect its interests during the execution of its business strategy.

Analysis of the results reveal that enterprise ontology is an important mechanism for explaining and understanding the complex nature of an enterprise as it interacts with internal and external entities. Examination of the properties of entities and nature and relationship between select resources provides clarity of their role, purpose, interdependency and failure effect. The resultant baseline forms the foundation for determining work effort required to support changes made to a business strategy. Security is applied at both the atomic and holistic level to ensure that the entire system does not shift into a state of chaos.

Conclusion

The focus of this research is to rethink the current approach to enterprise security. It achieves this in the following manner

[1] Development of an ontology that considers the nature of an enterprise as a complex system

[2] Development of a management framework that considers security in holistic terms

[3] Emphasizes fail-secure concepts by redefining security in terms of preventative, predictive and fail-safe models

[4] Disambiguation of security and defining specific business metrics and measures to improve security (expressed in terms of effort and investments)

[5] Shift away from equating security with protecting individual enterprise assets toward protecting business capabilities that possess strategic value and importance

[6] Many threats are complex in their action and therefore require an equally complex set of countermeasures by shifting focus from a simple cause and effect (linear) probabilistic model to a unified approach.

Several opportunities exist to enhance and automate the creation of enterprise ontology by examining the attributes and relationships of its resources and to eliminate (architectural) variability that drives complexity. The stability and security of a system is its ability to maintain an accepted level of equilibrium during the execution of its strategy. Such a condition is predicated on the belief that each resource has a known state that

is understood by it and other (interdependent) resources. Changes to a resource's internal condition would then trigger semantically based events that would indicate a probable failed state. Within a complex system, resources that are "ontologically aware" could trigger a self-preservation containment (fail-safe) event removing the need to collect and centrally maintain and analyze large amounts of syntax-based events.

References

Avižienis, A. et al. (2004) Basic Concepts and Taxonomy of Dependable and Secure Computing, In Proceedings of IEEE Transactions on Dependable and Secure Computing, January-March, 1 (1), pp. 11 - 33.

Barroero, T., Motta, G. & Pignatelli, G. (2010) Business Capabilities Centric Enterprise Architecture, *In the Proceedings of EAI2N 2010, International Federation for Information Processing, pp.32-43*.

Benzel, T. et al. (2005) Design Principles for Security [Online], Available from: http://cisr.nps.edu/downloads/techpubs/nps_cs_05_010.pdf (Accessed: 20 November 2013).

Burton, B. (2010) Eight Business Capability Modeling Best Practices, Gartner Research, ID Number G00175782, Gartner Inc.

Clark, D., Guba, E. & Smith, G. (1977) *Functions and Definitions of Functions of a Research Proposal*, Bloomington: College of Education Indiana University.

COBIT (2006) Control Objectives for Information and Related Technology (COBIT 4.0), IT Governance Institute.

Downes, J. & Goodman, J. (2010) *Barron's Finance and Investment Handbook*, New York: Barron's Education Series, Inc.

Deloitte Consulting (2012) Industry Print [Online]. Available from: http://www.deloitte.com/view/en_US/us/index.htm (Accessed: 20 September 2012).

Ekelhart, A., Fenz, S. & Neubauer, T. (2009) AURUM: A Framework for Information Security Risk Management, *In Proceedings of the 42nd Hawaii International Conference on System Science.*

Falliere, N., Murchu, L. and Chien, E. (2011) W32.Stuxnet Dossier [Online]. Available from:http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (Accessed: 4 July 2012).

Fenz, S. & Neubauer, T. (2009) How to Determine Threat Probabilities using Ontologies and Bayesian Networks, *In Proceedings of CSIIRW '09 ACM.*

Guevara, D. (2011) Australian Symposium/ITxpo Roundtable Exemplifies Strategic EA Challenges, *Gartner Research*, ID Number G00227138, Gartner Inc.

http://www.reliasoft.com (2012) BlockSim 8.0 [Online]. Available from: http://www.reliasoft.com/BlockSim/index.html (Accessed: 27 November 2013).

Jallow, A. et al. (2007) Operational Risk Analysis in Business Process, *BT Technology Journal*, January, 25 (1), pp. 168 - 177.

Kshetri, N. (2010) The Global Cybercrime Industry: Economic, Institutional and Strategic Perspective, London: Heidelberg Springer.

Kristen, R. et al. (2008) Formalizing Risk with Value-Focused Process Engineering [Online]. Available from: http://is2.lse.ac.uk/asp/aspecis/20080138.pdf (Accessed: 20 August 2012).

Lambrix, P. (2010) Ontology Alignment: State of the Art and An Application in Literature Search [Online]. Available from: www.ida.liu.se/~patla/talks/lambrix-rostock10.pdf (Accessed: 21 October 2012).

Martin, P. (2012) NASA Cybersecurity: An Examination of the Agency's Information Se-curity [Online]. Available from: http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf (Accessed: 8 July 2012).

McAfee (2011) Global Energy Cyberattacks: "Night Dragon" [Online]. Available from: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf (Accessed: 9 July 2012).

Meadows, D. (2008) *Thinking in Systems*, Chelsea Green Publishing.

Medicis Pharmaceutical Corporation (2012) Medicis [Online]. Available from: http://www.medicis.com (Accessed: 20 November 2012).

Milanovic, M., Milic, B. & Malek, M. (2008) Modeling Business Process Availability, *In the Proceedings of the IEEE International Congress on Services 2008 – Part I*, pp. 315 – 321.

Munro, K. (2011) RSA and the APT Attack [Online]. Available from: https://www.bit9.com/blog/2011/03/18/rsa-and-the-apt-attack/ (Accessed: 9 July 2012)

Nightingale, D. (2005) Enterprise Value Stream Mapping (EVSM) Workshop [Online]. Available from: http://lean.mit.edu/component/docman/doc_download/517-enterprise-value-stream-mapping-at-mit?Itemid=1 (Accessed: 20 August 2012).

Noy, N. & McGuinness, D. (2002) Ontology Development 101: A Guide to Creating Your First Ontology [Online]. Available from: ftp://ftp.ksl.stanford.edu/pub/KSL_Reports/KSL-01-05.pdf.gz (Accessed: 24 October 2012).

O'Connor, P. and Kleyner, A. (2012) *Practical Reliability Engineering*, John Wiley and Sons, Inc.

Peterson, G. (2007) Security Architecture Blueprint [Online]. Available from: http://www.arctecgroup.net/pdf/ArctecSecurityArchitectureBlueprint.pdf (Accessed: 20 August 2012).

Protégé (2012) Protégé, the National Center for Biomedical Ontology, National Institute of General Medical Sciences [Online]. Available from: http://protege.stanford.edu/download/registered.html (Accessed: 20 September 2012).

Rebovich, G. (2011) Systems Thinking for the Enterprise. In: Rebovich & White, ed. 2011. Enterprise Systems Engineering: Advances in the Theory and Practice. New York: CRC Press.

Renkema, T. (2000) *The IT Value Quest: How to Capture the Business Value of IT-Based Infrastructure*, New York: John Wiley & Sons, Ltd.

Sackmann, S. (2008) Assessing the Effects of IT Changes on IT Risk – A Business Process-Oriented View [Online]. Available from: http://ibis.in.tum.de/mkwi08/17_IT-Risikomanagement_-_IT-Projekte_und_IT-Compliance/05_Sackmann.pdf (Accessed: July 30 2012).

Simmonds, A., Sandilands, P. & Ekert, L. (2006) *An Ontology for Network Security Attacks*, Sydney: University of Technology.

Smith, M. (2010) The Gartner Business Value Model: A Framework for measuring Business Performance, *Gartner Research*, ID Number G00175097, Gartner Inc.

Smith, B. & Welty, C. (2001) Ontology: Towards a New Synthesis, *In Proceedings of the FOIS'01 ACM,* October.

Sterman, J. (2000) *Business Dynamics: Systems Thinking and Modeling for a Complex World*, Boston: McGraw-Hill Companies Inc.

Weill, P. & Broadbent, M. (1998) *Leveraging the New Infrastructure: How Market Leaders Capitalize on Information Technology*, Boston: Harvard Business School Press.