

WHITE PAPER

An Enterprise Security Program and Architecture to Support Business Drivers



CONTENTS

3	Introduction
4	Information Assurance
6	Sherwood Applied Business Security Architecture
9	Enterprise Security Architecture: Establishing the Business Context
14	Creating a Model of Business Risk
15	Trust Models
16	Threat Models
17	Safeguards
19	Using a Business Risk Model to Drive Security Architecture
20	Relevance to Cybersecurity
23	Conclusion

INTRODUCTION

Many organizations find that their security controls prevent them from getting something done or reduce their effectiveness. Conversely, an organization may question whether there is sufficient protection for information to be shared with a new business partner, customer, or the general public.

*If a critical system is compromised,
what will be the business impact?*

Security practitioners are challenged to consider security in the context of the business and understand the duality of risk: some risks represent business opportunities and should therefore be accepted. However, risk avoidance is a common practice in IT organizations, where security expenditures, policies, procedures, and technologies are not proportional to the risk appetite of the business.

When security controls become overly intrusive to employees of a business and, in fact, impede business operations, individuals will seek the means to bypass the controls. This desire to avoid security is due to a perception that security is an obstacle. As a result of this security avoidance, new risks are introduced; however, these are not known to the security team and cannot be monitored and managed. This situation describes a common struggle faced by most organizations. Organizations strive to achieve an appropriate balance between security controls to protect business information and allowing their employees to be productive and share information easily. Achieving this balance requires information assurance.

This white paper provides an understanding of information assurance and presents the case for leveraging enterprise security

For a security program to be effective, it must demonstrate value to the business while avoiding traditional pitfalls associated with the perception of security being an inconvenience and an obstacle to business operations.

IT security deals primarily with the confidentiality, integrity, and availability of information and provides mechanisms to protect these aspects.

architectures to meet an organization's need for information assurance. The approach is derived from the Sherwood Applied Business Security Architecture (SABSA) methodology, as put into practice by Hitachi Systems Security Inc.

This white paper is intended for senior executives who are trying to rationalize an appropriate balance between protection and availability of information that supports the business. The report will also help security practitioners (in particular security architects) understand how to align security initiatives with business goals to deliver an effective security program.

INFORMATION ASSURANCE

- *Information Assurance* relates to the management of risk and security regarding use, processing, storage, and transmission of data. Information assurance is a much broader category than information security, which predominantly focused on IT security controls and processes. When information is compromised, the result is a change in state of one of these aspects.
- *Confidentiality* ensures that privileged or sensitive information is accessible only to individuals with a valid requirement to view and access the information. It is particularly important when concerning personal information, intellectual property, and classified or sensitive information in a government context.
- *Integrity* refers to a lack of corruption in data or overall consistency. When integrity of information is compromised, it creates a lack of trust wherein data may have been manipulated, changed, or deleted.

- **Availability** relates to having access to authorized information when it is required. Should information be affected so it cannot be accessed when needed and authorized, then availability has been compromised.

Information risk arises when the confidentiality, availability, or integrity of data can be compromised. To mitigate risk, controls can be developed and implemented to provide increased assurance of information. A control is a safeguard or countermeasure designed to avoid, minimize, or counteract risk.

The practice of information assurance relies on identification of risk and application of appropriate controls. However, over time, this practice has become categorized as *risk adverse* and seen as an impediment to business effectiveness. Information security professionals are labeled as obstacles to successful implementation and delivery of IT solutions. The resulting business culture is reluctant to involve and solicit input from IT security teams, because the input can create business risk for a project and delay implementation. This view comes from the practice of creating a risk-avoidance approach to information security based solely on technical threats, identification of risk, and the use of as many controls as possible to mitigate risk. The end result of this practice is a security program that fails in its effectiveness, given reluctance at an organizational level to involve security in early stages of projects and planning. True information assurance practices must also recognize the value and importance of making information available and establishing safe information-sharing practices.

When faced with these challenges, many organizations may default to implementing more security controls to minimize

According to the US Intellectual Property Commission Report (IP Commission, 2013), hundreds of billions of dollars are lost each year to the theft of intellectual property. Increasingly, this theft is the result of cyber-attacks against United States' electronic infrastructure.

Sophisticated samples of malware have been discovered in recent years, with demonstrated capability to attack SCADA control networks and negatively impact critical infrastructure. The two most notable examples are *Stuxnet* and *Flame* (Klochender, 2013). Together, all of these examples indicate a failing in existing information assurance practices and a rise in the sophistication and capabilities of cyber-adversaries.

vulnerabilities and deny cyber-adversaries access to systems. An approach focused solely on controls will ultimately prove unsuccessful given the resourcefulness and capabilities of malicious threat actors, as demonstrated in the examples above.

Organizations across multiple sectors and varying levels of government there has been identified a common thread; while most organizations are security conscious and acknowledge the need for good IT security practices, they lack the necessary knowledge needed to build effective security programs.

Security programs should be designed to provide appropriate protection for information and information assets. This protection should be tailored to the environment, which requires identification of what information is most vital to an organization. Without a clear understanding of priorities for information and information security, organizations are incapable of prioritizing control improvements. A lack of a structured security architecture impacts all aspects of an organization's IT security program, including threat monitoring, vulnerability management, identity management, and incident response just to name a few. Effective security operations require effective security architecture

SHERWOOD APPLIED BUSINESS SECURITY ARCHITECTURE

When security is found to be cumbersome or intrusive into business practices, loopholes and shortcuts are taken to bypass implemented controls, creating increased risk that is not accounted for and easily capitalized upon by threats seeking to compromise the confidentiality, integrity, and availability of data. The Sherwood Applied Business Security Architecture (SABSA) methodology for an enterprise security architecture

and program can be leveraged to address this shortcoming (Sherwood, et al., 2009).

In essence, the SABSA approach is positioned on making security a business enabler rather than an obstacle or avoidable inconvenience. The SABSA approach creates an understanding of an organization's business objectives and provides a structured approach to designing a security program that supports these objectives. Security does not hinder business objectives, but instead provides assurances around operational risk that could negatively impact the business and enables the organization to take on new strategic opportunities.

It is necessary for organizations to accept risk to do business and be effective. Embracing the right type of risk has the potential of leading to good fortune for a business.

An important element to consider, when selecting an architectural framework for security, is that many organizations already have an established IT architecture program to facilitate delivery of IT projects. Existing architectural frameworks include the Open Group Architecture Framework (TOGAF) and the Zachman Framework for Enterprise Architecture; however, such frameworks do not traditionally address security requirements. Furthermore, many organizations implement service-management programs to manage and operate IT systems and services. The Information Technology Infrastructure Library (ITIL) is an example of such a service-management framework.

SABSA is unique among architectural frameworks in that it does not seek to replace or interfere with these existing frameworks and practices, but instead integrates with them and provides tools necessary to align and support existing architectural programs. This ease of alignment with existing frameworks and

SABSA is a unique approach to information assurance because it seeks to align security programs with an organization's fundamental business objectives and drivers. In doing so, the SABSA approach treats risk as something that cannot only hinder a business, but also can enable new opportunities.

For each of the architectural views in Figure 1, SABSA encourages security architecture to consider:

- **What are you trying to protect at each layer? (Assets)**
- **Why are you protecting these assets? (Motivation)**
- **How will you achieve your objective? (Process)**
- **Who is involved in applying security? (People)**
- **Where are you applying security? (Location)**
- **When are you applying security? (Time)**

the focus on leveraging security as a business enabler are key criteria that affected Hitachi Systems Security Inc.’ decision to use SABSA as a framework for delivering enterprise security architectures.

To make security relevant to all stakeholders in an organization, the SABSA framework introduces a layered approach to architecture. Each layer corresponds to a different player’s view in the organization as it relates to specifying, designing, constructing, and operating a security architecture (as shown in Figure 1).

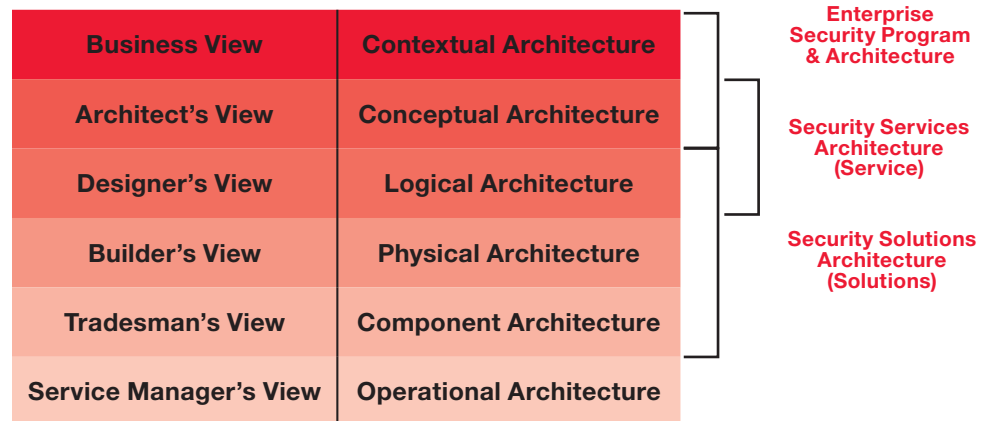


Figure 1. The SABSA model for security architecture

SABSA provides the theory and background knowledge essential to delivering business-driven security architectures; however, the practice of delivering the architecture is left to the security practitioner.

ENTERPRISE SECURITY ARCHITECTURE: ESTABLISHING THE BUSINESS CONTEXT

A business-driven approach to enterprise security architecture means that security is about enabling the objective of an organization by controlling operational risk. This business-driven approach becomes a key differentiator from existing security practices that are focused solely on identifying threats to an enterprise and technical vulnerabilities in IT infrastructure, and subsequently implementing controls to mitigate the risks introduced.

The term security will carry very different meanings to different organizations. For example, consider security as it relates to a military organization and security related to an online retailer that processes credit card information. The business models for these two organizations will be very different and, as a result, the security programs should be unique and relevant to their underlying businesses.

A military organization may determine that the most critical asset to protect is the life of its soldiers as they are engaged in military operations. To provide assurance, complex security architectures are needed to protect information and information systems that could impact the soldiers' safety. Solutions could include ensuring that logistic systems that manage the delivery of supplies, food, and ammunitions remain available, and that data integrity is protected to protecting confidentiality of mission plans and military intelligence that, if compromised, could cause considerable harm to war fighters.

An online retailer is likely most concerned with compliance with standards set by the payment card industry. These standards

A purely threat-based approach to risk management fails to enable effective security and business operations.

Developing a security architecture begins with an understanding of the business—which is achieved by defining business drivers and attributes.

are tailored to protect the confidentiality of personal information and the integrity of transactions. An online retailer may have lower thresholds for availability than a military logistics system. The needs for confidentiality, availability, and integrity of data must be balanced and appropriate to the business activity.

Developing a security architecture begins with an understanding of the business—which is achieved by defining business drivers and attributes. A business driver is related to the organization's strategies, operational plans, and elements considered critical to success. A business attribute is a key property of the strategic objectives that need to be enabled or protected by the enterprise security program. An organization's senior executives, who set the long-term strategy and direction of the business, can typically provide knowledge regarding business drivers. The drivers are often reflected in an organization's mission and vision statements.

Consider the military organization example, which may have a strategic objective of *operational excellence*. This business driver can be distilled into relevant attributes that require assurance to satisfy the overarching business driver. The online retailer may have a strategic objective of being *customer focused*, as expressed in their vision statement to provide a superior online shopping experience.


Business attributes can generally be identified through an understanding of the business drivers set by the top levels of an organization. Security architects will often conduct structured interviews with senior management to identify business attributes by determining the essence of what is conveyed by high-level business drivers. In the example of the business driver *operational excellence*, the executives might be referring to the availability, reliability, and safety of their operations and

resources. In this case, the business attributes defined are *available, safe, and reliable*.

Each attribute is then linked to the business driver that they support. This pairing of a business driver and attribute results in the creation of a proxy asset. Building on our example, a sample proxy asset is *operational excellence* with the attribute of *available*. Each proxy asset is owned by the organization and is assessed as having value to them. The fact that the proxy asset has value sets the requirement that it should be protected. The value of these proxy assets is difficult to define given that they are often intangible and exist at a very high level. Despite being unable to assign a monetary value to a proxy asset, it is still possible to identify risks that may act against the asset. Our example online retailer may have attributes of *confidential, reputable, and error-free*.

An inventory of proxy assets can be maintained by the security architect and will be considered as key assets to the organization. This is later used to conduct a business threat and risk assessment to identify risks to the business. Through a business threat and risk assessment, the sometimes-competing aspects of confidentiality, integrity, and availability can be reconciled. When the overall objective and needs of a business are understood, through proxy assets, then impact can be understood as it relates to confidentiality, integrity, and availability. Understanding the business helps prioritize which of these elements is most important and which aspects of the business are most in need of protection.

Traditional threat-based risks are those that can be mitigated via a control because they would result in the loss of value. Many organizations rely on threat risk assessment to create



Through a business threat and risk assessment, the sometimes-competing aspects of confidentiality, integrity, and availability can be reconciled.

The implementation of controls sometimes does not offer protection for what is truly important to the business.

an inventory of threats that may have a negative impact on the business. Threats are then mapped to vulnerabilities that, when exploited, result in a compromise to the organization's business. Managing this risk often relies on the deployment of security controls that offer a form of mitigation. For example, an external website that has a technical vulnerability that could result in a threat that exploits this vulnerability, such as a denial-of-service attack, which would render the website inaccessible. Threat-based risk analysis would identify the threat and provide recommendations on control improvements to decrease the risk. This may include deployment of a web-application firewall to provide intrusion-prevention capabilities, increased network monitoring, deployment of additional firewalls, and software upgrades to reduce the vulnerability.

The traditional approach, described above, successfully identifies risk based on analysis of possible threats and provides the means of mitigating that risk. The relation of the risk to business impact, however, is missing in this approach. Perhaps the server is used for testing with a small number of business partners, and denial of service is not a risk of importance.

The implementation of controls sometimes does not offer protection for what is truly important to the business. Controls can increase complexity in the network and incur costs that could have been avoided. When identifying risk using only threat-based approaches, key information, which could have informed a security architect on where to prioritize control improvements, is likely missing. Another problem with threat-based approaches is that they do not consider the potential opportunity that can be realized when embracing risk.


Consider the non-traditional idea that risks can also be

categorized as opportunity-based. This perspective is lacking from traditional information assurance practices. An opportunity-based risk can increase the value of an asset. This approach enables us to understand the duality of risk. Some risks should be mitigated; others might be accepted as something that cannot necessarily be avoided. Businesses always operate with some level of inherent risk.

When a business and security architects understand the duality of risk, they can also focus on risk acceptance rather than just risk avoidance. To this end, the organization develops key performance indicators (KPIs) and key risk indicators (KRIs). KPIs are measures of the value and performance of business attributes in the context of the business driver. KRIs are measures of risk, and they establish risk thresholds to provide early warning when a risk will exceed an organization's risk tolerance.

In the military example, we identified *operational excellence* as a business driver and *available* as an attribute. Developing a KPI regarding the availability of operational systems would allow the organization to measure the availability and uptime of a key business application. The performance of this application could be tracked over time to ensure that it remained available and supported the business driver of *operational excellence*.

The same example could be considered from a different angle and result in development of a KRI. A KRI differs from a KPI, in that it establishes a threshold or condition that creates a warning state. Monitoring of KRIs provides an indication when risk is about to exceed established tolerance levels. In our example, a KRI might enable ongoing measurement of the time that an application is inaccessible. The system may be inaccessible due



Some risks should be mitigated; others might be accepted as something that cannot necessarily be avoided. Businesses always operate with some level of inherent risk.

Regardless of the indicator selected (KPIs or KRIs), when considered in the context of business drivers and attributes, it becomes possible for security to have sufficient information to consider risk in the context of business objectives.

to technical circumstances such as network failure, software updates, or other IT incidents. Measuring the time that an application is inaccessible will facilitate identification of an established threshold that sets unacceptable behavior. When the key business application approaches this threshold, alerts can be generated to warn that the established risk tolerance is soon to be exceeded.

In the online retailer example, the attribute *error free* can apply to the processing of financial transactions. To provide a consistent experience for users and to maintain customer confidence, the online retailer wants to ensure that any transactions are without error. A KRI can be created to capture any dispute of a financial transaction due to a potential error. It is likely that a very low threshold would be established and any errors would trigger appropriate response to investigate and remediate the cause of the error.

Regardless of the indicator selected (KPIs or KRIs), when considered in the context of business drivers and attributes, it becomes possible for security to have sufficient information to consider risk in the context of business objectives. This understanding of risk will contribute to an overarching model of business risk, which is needed for a security architect to successfully develop security architecture at an enterprise level.

CREATING A MODEL OF BUSINESS RISK

A model of business risk provides a mechanism for quantifying risk and ensuring that it remains relevant to business drivers and attributes (as previously described). The business-risk model builds on the understanding of risk, centered on the established

proxy assets as well as KRIs and KPIs. In addition to the proxy assets and KPIs and KRIs, there are other models that also must be developed and understood to complete the business-risk model:

- Trust models and business relationships
- Threats operating against the business
- Safeguards that have been implemented

This approach is similar to a threat risk assessment—the difference is that a threat risk assessment measures the risk to a system or IT environment; an enterprise security architecture measures risk to the proxy assets that represent the organization’s business.

A threat risk assessment measures the risk to a system or IT environment; an enterprise security architecture measures risk to the proxy assets that represent the organization’s business.

TRUST MODELS

Trust needs to be considered in context of the overall business as a business attribute, not a technical one. Whenever two or more entities are required to interact and exchange information, trust must first be established between them. Trust can be established through registration of the entity by the other. The registering entity will then trust the entity that has been registered, based on assurance mechanisms. The levels of assurance required to establish this trust vary, based on the degree of risk involved.

As an example, consider a shopkeeper selling lottery tickets to a customer. For the shopkeeper to trust the customer, they require a valid form of identification, such as a driver’s license, to validate the customer’s age. The decision to require the driver’s license is based on a risk decision taken by the shopkeeper on whether the individual appears of age or not. Conversely,

Understanding business risk requires that relationships internal and external to a business are properly understood.

the customer must trust the shopkeeper as a valid merchant authorized to sell lottery tickets. This trust is established through the clear display of the lottery license issued and validated by the government. Once these assurances are validated, then the shopkeeper and customer establish a two-way trust relationship to complete the transaction.

Understanding business risk requires that relationships internal and external to a business are properly understood. Evaluation is required to gather information related to the criticality of a relationship, the sensitivity of information shared, and existing methods of assuring trust between the parties involved in a relationship. A security architect can explore the relationships—both internal and external to an organization—to identify points where information is exchanged. This can be used by a security architect to layer logical relationships to the physical IT environment, to prioritize placement of controls that assure trust and protect information as it is exchanged as part of business relationships.

THREAT MODELS

Threats are entities or things, operating against a business, that cause damage or harm to an organization. Understanding threats is an important step in developing awareness of business risk. Typically, safeguards are implemented to mitigate damage caused by a threat that is exploiting a vulnerability. A threat may be a deliberate action taken by an entity or it may be accidental, based on an unintentional realization of a scenario that creates risk. Natural hazards, such as fire and flood, are threats that may impact a business. Understanding these threats, the likelihood of them operating against a business, and the gravity

of consequences should they succeed, helps in prioritizing threats based on their impact and likelihood of being realized.

In the case of the example military organization, a threat to availability may materialize from a hostile government agency or military that would seek to disrupt the availability of key systems essential to effective military operations. The online retailer would not necessarily be concerned with military threats, and would instead consider organized crime as a threat that would seek to abuse the technical application in the retailer environment for the purposes of financial gain. This threat may include gaining access to confidential customer data for identity theft or exploiting application vulnerabilities to receive goods without paying full price. The threat model can be made relevant to the organization by considering threats that affect the proxy assets defined earlier in the process.



SAFEGUARDS

The final piece required to establish the business risk model is an understanding of existing safeguards along with any gaps that exist in mitigating risk associated with threat activity. Industries follow various standards of best practice and frameworks to

The final piece required to establish the business risk model is an understanding of existing safeguards along with any gaps that exist in mitigating risk associated with threat activity.

Once a control framework is selected, a review of the controls can be undertaken along with assessment of the maturity level for each control, and the extent to which it is implemented in the business.

assess their relative maturity regarding security controls and safeguards implemented to mitigate risk.

A popular general purpose control framework is ISO 27002, which is provided by the International Organization for Standardization (ISO). This standard provides industry best practices for information security management. Other control frameworks specific to industries include the North American Electrical Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard and the International Society of Automation (ISA) standards. Selecting the appropriate framework is an important step in review and identification of relevant gaps. Each business will have a unique set of controls particular to their industry and the regulated protection required. Once a control framework is selected, a review of the controls can be undertaken along with assessment of the maturity level for each control, and the extent to which it is implemented in the business.

Once all data around risks, relationships and trust, threats, and control effectiveness have been gathered, the inherent risk to a business can be described and represented. An initial assessment is undertaken where the business impact of a risk being realized is considered, irrespective of any existing controls, to quantify the severity of risk. Based on this understanding of the inherent risk, a security architect can identify areas for improvement that will manage risk and establish acceptable thresholds. Inherent risk is a measure of the risk to the enterprise prior to any controls being implemented.

Risk can be classified on a scale tailored to meet an organization's need; however—fundamentally—risk will be quantified as negligible, acceptable, significant, or severe. In the case of negligible risk, no action is required, whereas acceptable risk

requires monitoring to ensure that it remains at an acceptable level. Significant and severe risks require action to establish an appropriate risk threshold in which the business is comfortable operating, to maximize opportunities.


The resulting risk score is known as residual risk, which is the risk that remains after security controls and improvements are selected, approved, and implemented in an environment. Improvements to controls can be simulated and new risk scores can be calculated to develop risk-reduction strategies. This process shows how security improvements can affect enterprise-wide risk.

Because various improvements carry different complexities and cost, multiple models can be constructed to show options and potential benefits over time as control improvements are made. This approach allows an understanding of risk appetite and provides the overall business-risk model.

USING A BUSINESS RISK MODEL TO DRIVE SECURITY ARCHITECTURE

Once a business risk model has been completed, a security architect can leverage this information to create logical security services. A logical service is specified independent of any physical mechanism that might be used to deliver the service. Most importantly, a logical service is driven from the business attributes and the business-risk model.

A security service is therefore a combination of security controls that work together to support the delivery of a valued business service. A number of security services can be developed to



A security service is a combination of security controls that work together to support the delivery of a valued business service.

The added benefit of developing security services based on the business-risk model is that full traceability can be maintained, demonstrating that security initiatives are tied to supporting an organization's business and effectively managing both threat- and opportunity-based risk.

provide *defence in depth* and increase the overall assurance of information that is important to the business. Security services that can be created may include threat management, vulnerability management, and network access. These services will form part of a security-services catalogue and, as a result, services can be selected and implemented based on the needs of a specific business initiative. Unlike traditional security controls, these services are derived from business drivers and attributes, and they provide traceability to the business objectives.

The services to be designed will draw on the information gathered in the business-risk model, particularly the understanding of relationships (expressed as physical boundaries where information is shared), threats that are operating against the environment, and opportunities for control enhancements to mitigate the risks introduced by threats. The added benefit of developing security services based on the business-risk model is that full traceability can be maintained, demonstrating that security initiatives are tied to supporting an organization's business and effectively managing both threat- and opportunity-based risk.

RELEVANCE TO CYBER SECURITY

Although the concept of enterprise security architecture does not provide a concrete technical tool with which to counter advanced persistent threats or zero-day attacks, it provides a critical tool to identify and assess assets of value to an organization. This step is often missing when developing security programs, which can lead to deployment of controls without a proper understanding of how they can hinder or support the overarching business objectives.

In the two examples, the military organization and the online retailer, both are likely to have an internet-accessible website. The purposes of these websites would be very different. For the military, it likely provides general information at the unclassified level to the general public; it would not likely be used for operational missions and would be in a separate network segment from critical operational systems. The online retailer, however, would use the website as a front-end to their e-business, where the website provides customers with the ability to browse and purchase merchandise. If both organizations have an enterprise security architecture, then they are better equipped to respond to, and deal with, threat activity when it materializes against their website.

In the event of a zero-day attack against their web server, the military would realize that the attack did not affect any critical information and was not related to a key relationship that was foundational to success of the organization. During incident response, the effort and tools used to respond would be appropriate, and control improvement would be balanced, based on cost, impact, and risk tolerance. Although the reputation of the organization may be damaged should the information become public, the overall business impact would be minimal. The online retailer, however, would need a much different response based on their business needs. Furthermore, the logical security services we alluded to would be geared toward protecting confidentiality and ensuring error-free processing.

Although the discussion of logical-service design falls outside of the scope of this report, consider briefly the concept of vulnerability management. The online retailer would likely perform regular web application assessments and vulnerability testing against its website and web application to protect customer



If both organizations have an enterprise security architecture, then they are better equipped to respond to, and deal with, threat activity when it materializes against their website.

Attempting to counter emerging cyber threats without a clear understanding of the business needs of an organization will result in ineffective security controls and practices.

data appropriately. The military organization, also implementing a vulnerability-management program, would most likely scan the website on a much less frequent basis and focus efforts on securing mission-critical systems, requiring high availability.

An enterprise security architecture helps organizations identify assets of critical importance. Attempting to counter emerging cyber threats without a clear understanding of the business needs of an organization will result in ineffective security controls and practices. When security is considered in the context of the enterprise, as both an enabler and means of assuring business success, control improvements can be tailored to the environment to address more sophisticated and complex threat scenarios.

In the cases of ten million new malware instances every six months, intellectual property theft in the billions of dollars, and sophisticated intrusions such as Stuxnet, organizations are often incapable of prioritizing security initiatives and default to technical solutions without proper identification of critical assets and information. The cyber-challenge requires that organizations be better equipped than the threats acting against them, and an enterprise security architecture provides this capability.


CONCLUSION

For information assurance to effectively strike an appropriate balance between protection of information and making the correct information easily assessable to authorized parties, an enterprise security architecture needs to be developed with a focus on business goals.

An enterprise security architecture should provide a means of mitigating risk while also supporting the business to pursue new opportunities.

The approach described in this article provides security practitioners and senior executives with the knowledge and foundational information to connect security performance to business performance. As IT threats facing an organization continue to grow in volume and variety, a reasonable approach is needed to address threats while continuing to support the operations of the business.

Organizations that focus solely on eradication of threats and vulnerabilities when developing security architecture risk creating an environment where security becomes an obstacle to operations. A business-driven approach to security architecture helps organizations prioritize where controls are needed to protect critical information and define what level of risk is acceptable.



An enterprise security architecture should provide a means of mitigating risk while also supporting the business to pursue new opportunities.

 **Hitachi Systems Security Inc.**

955 boul. Michèle-Bohec, Suite 244, Blainville (Québec) J7C 5J6 Canada

Tel: +1 450-430-8166 Fax: +1 450-430-1858

www.hitachi-systems-security.com