



Introduction to Business Security Patterns

Efficient and effective security is an integral part of a business delivering value. Institutions require security for their own operations and for their interactions with customers and partners.

An IBM White Paper

Contents

- 1. INTRODUCTION..... 1
- 2. RATIONALE 2
- 3. UNDERSTANDING RISK 3
- 4. SECURITY PATTERNS..... 4
- 5. SECURING YOUR INSTITUTION..... 15

1. INTRODUCTION

Institutions face risks as part of doing business. There are inherent risks in their operations and in their interactions with customers and partners. Identifying and understanding the relationships between these risks and security solutions is essential to employing effective security to address these risks. Business security patterns establish a powerful methodology to identify and understand these relationships to help maximize the value of security investment.

This document presents an introduction to business security patterns. It is intended for use by the Chief Information Officer, Chief Security Officer, as well as by any individual or organization within an institution that is responsible for information technology and security.



The document begins by discussing risk and security from a business perspective. The document then presents the rationale supporting business security patterns. The pattern concept is discussed and the five specific business security patterns are introduced. The ensuing sections give an overview of each pattern individually, culminating with an example scenario employing all of the patterns. The patterns are then considered against the backdrop of a set of common attributes that in turn are used to further distinguish each pattern from a risk and security solution perspective. The document concludes with a discussion of how the patterns and the values of their attributes can then be used to identify specific business risks, appropriate security solutions, and help to determine an effective course of action to realize value for the business.

2. RATIONALE

Establishments exist to create value in products and services. Delivering value requires the application of physical, logical and privacy boundaries to users, processes and resources.

These boundaries should be secured in a cost-effective manner. However, this is not easy to do. Given that most businesses already have in place an extensive set of users, processes and resources few real opportunities exist to apply a “clean sheet of paper” approach, as security plan implementations can be disruptive to existing operations. Therefore, organizations have struggled for decades with the question of *“How do you apply the right security resources to manage the business risks?”* And recently, with the increased focus on security in governments, standards bodies, trade practices and regulation, determining and cost-effectively managing risk has become a predominant thought for many data centre managers.

Security is not just a product, and it is not just a service. It is a condition that is expected to be embedded in the process of creating value. Security encompasses diverse issues. It can be considered as physical security (guards, guns, badges), security products, (firewalls, intrusion detection systems and security management tools), as part of managed security services, or simply, as embedded attributes of products such as operating systems or data repositories.

Security is never absolute. There is no such thing as complete safety or complete freedom from doubt or fear – people and organizations always face risks. Some risks can be eliminated, some can be reduced, and some can be accepted. There should always be an expectation that any security can be breached. An organization is “secure” when it understands the risks, and is able to manage them so that, the costs used to reduce risk are commensurate with the expected business value. As a provider of IT Services, you have to balance the cost of a security with the benefits to your business.

3. UNDERSTANDING RISK

For the purposes of this paper, a risk is the possibility that something negative or undesirable will happen. A business risk is the possibility that something undesirable will happen to the business, its customers or an entity the business depends on. Typically, most business risks are quantified in economic terms such as lost revenue, wages, or damage to the brand. Lowering the probability that the business value will be decreased or lowering the consequences or the economic loss of an incident can reduce business risks. The different types of risks and the variety of ways in which businesses can manage these risks are depicted below.

Risks to the Institution

Asset Risk – Theft, destruction, or corruption of business assets. Denial of legitimate access to business assets.

Identity Risk – Impersonation of legitimate users.

Infrastructure Risk – Subversion of business systems; circumvention of protection measures.

Custodial Risk – Failure to protect assets belonging to third parties, including personal information about individuals.

Compliance Risk – Liability for failure to comply with laws and regulations requiring security and privacy protection.

Risk Management Options

Transfer – A business can transfer risks to other parties.

Indemnify – A business can recover the cost of a risk through arrangements with third-party specialists.

Mitigate – A business can mitigate risk either by reducing the probability that an adverse event will occur or by reducing the consequences resulting from the event's occurrence.

Avoid – A business can choose not to engage in activities which create certain types of risks.

Accept – A business can choose to accept the consequences.



There are multiple risk management options for any given risk. The complex nature of risks, multiple risk management options and business needs highlights the need for a consistent security methodology. Business security patterns provide a security methodology that can be used to derive security solutions that cost effectively mitigate risk. The next sections of this paper define and explain business security patterns.



4. SECURITY PATTERNS

IBM has uncovered a collection of business security patterns through extensive primary research and experience with institutions in financial services, government, manufacturing, health, transportation, retail and other sectors. Interviews conducted in early 2003 were held with large, medium, and small institutions in the public, private, regulated and non-regulated sectors. These interviews have coalesced ideas from academia, research and business (including the huge internal infrastructure within IBM) as part of the maturing of IT security in general.

During interviews, consistent themes emerged independent of the industry or enterprise.

Across the board, institutions struggled to organize their users, resources and processes effectively in order to create a secure yet cost-effective environment. In these discussions, IBM determined the existence of a set of repeatable business needs surrounding the enforcement of boundaries, risk mitigation, and security technology. These needs can be related to a set of business attributes found in every institution.

Business security patterns are used to identify and understand the relationships between business goals, business risks and security solutions. The five major business security patterns are:

Web Presence

Business to Consumer

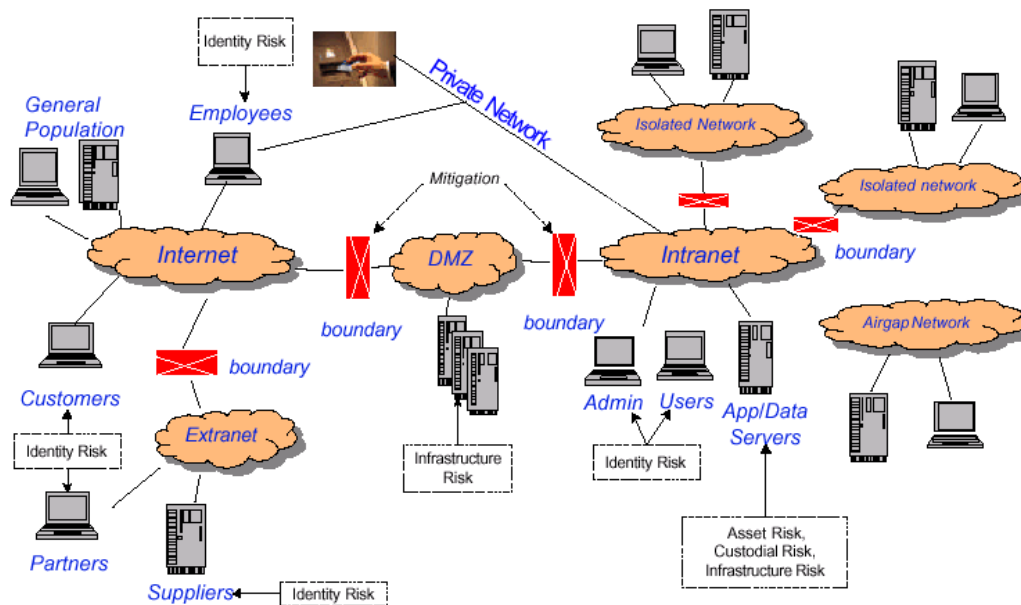
Business to Business

Operational Security

High Assurance

The value of the patterns derives from the mapping of business and risk parameters into organized structures that provide a template for effectively implementing security. By evaluating your institution using business security patterns, you can create a repeatable methodology to help apply appropriate and cost-effective security to your enterprise. Each business security pattern is used to describe an aspect of a business process that has a level of associated risk. By combining multiple security patterns, you create a security solution addressing multiple business needs.

The graphic below depicts a representative customer environment that is typically composed of legacy systems and emerging business systems. The sheer complexity and interconnectivity inherent may lead to unidentified security exposures. It is imperative to be able to decompose the complexity into a finite set of business usages that identify the “who, what, where, how, why, and when” aspects of security. Business security patterns overlaid on the topological view of business systems below provide the powerful framework to organize security decision points, business value, and business drivers comprehensively.



Web Presence

The simplest pattern start with is Web Presence. Web Presence is typically an Internet-based information portal, or as an aspect of a business, it is the dissemination of customer facing, non-transaction-oriented business information. The goal of Web Presence is to provide Internet-based access to a business' public information. The key operational characteristic of Web Presence is the information shared is public and the value of the information derives from its availability and dissemination.

The basic goal of security in the Web Presence pattern is the protection of the integrity and availability of the information to be disseminated. The business has little control over the access points, which are web browsers running on traditional personal computing devices, or pervasive devices such as PDAs and Internet-capable cell phones. The lack of security for the access point has low risk associated with it because the information is public.



Web Presence presents limited opportunity for attackers. The major risk for a business arising from this pattern is harm to the business' brand image and value. The threats include:

- (1) The data might not be available due to a denial of service attack or the destruction of the information being presented or
- (2) the data may be corrupted as would happen in a site defacement attack.

There are two subcategories within Web Presence:

Isolated from core business: If the Web Presence does not have connectivity to the business' intranet, access to other business systems does not exist. Therefore, the only concern is the integrity and availability of the data being presented.

Integrated with core business: If the Web Presence has connectivity to the business' intranet, security vulnerabilities may lead to unintended network and systems access, termed collateral access, that result in additional exposures in Operational Security. However, these risks, threats and vulnerabilities are addressed in the context of Operational Security. In many cases, the risks, threats, and vulnerabilities are part of a composite set pattern that includes Web Presence and Operational Security.

As part of the strategy to maintain the availability and integrity of the data and contain the additional exposures to operational security, many companies deploy multi-level security barriers to create a "neutral zone" between a business' intranet and an un-secure network such as the Internet. The neutral zone is often referred to as a demilitarized zone (DMZ). The DMZs are bounded by firewalls that protect the data and attempt to mitigate denial-of-service attacks.

High-availability server solutions inside the DMZ also help mitigate availability risks.



Business-to-Consumer

The Business-to-Consumer (B2C) pattern encompasses a business' ability to conduct transactions with or on behalf of customers over networked systems. The B2C operations provide access for individuals to engage in online commerce and to manage data such as accounts, e-mail, collaboration, and employee benefits. Businesses that must deliver tangible or long term value (cash, tickets, vouchers, and games) to the customer typically require the use of physically secure endpoints. The physically secure endpoints are built from purpose optimized devices. However, the basic business goal of the B2C pattern is to preserve the value of the brand and business while enabling transactions or subscription-based services. Therefore, businesses described by the B2C pattern are web retailers, financial services, benefits administrators, and subscription-based services such as e-mail, telematics, personalized information, and so forth.

There are four subcategories for B2C:

Store Front: the business is engaged in transactions with customers, there may not be a long-term relationship, and the value of any one transaction is limited.

Subscription-Based Services: the business engages in a long-term relationship with the customer. The data is persistent, the access to other business systems is limited and the privacy and data separation concerns are higher.

Purpose Optimized Devices: the business delivers tangible value (includes games) to the customer by way of a special-purpose access point. The access to other business systems is limited because the access point is a fixed function device. The physical protection of the access device is an additional security concern.

Employee-to-Business: The employee (a consumer in this context) may sit within the corporate infrastructure increasing the risk because of available access to collateral systems. The privacy of the data associated with employee-to-business should be ensured by appropriate access and data separation controls.

A fundamental characteristic of B2C is that the user must be known through some registration process and yet the authentication mechanisms for verifying a user's identity are limited. The common user identification methods are user identification and password, smartcards, browser cookies, or third party user authentication. In situations where third-party authentication is required, the scenario resembles a parallel B2C transaction with a business-to-business (B2B) transaction occurring in the background. The assets to be secured are: personally identifiable information, account access information, information presented to the consumer and the links between the business and the consumer.



Aside from the identity of the user, the B2C pattern has additional, specific basic attributes. B2C transactions involve the exchange of personal information, financial data, personalized subscription based information, or data with long term value (for example, games, movies). Therefore, the business should provide transaction-based protection of the data and identities. The value for any one transaction is limited although the accuracy is important.

Industries and governments in this pattern increasingly regulate privacy concerns. Overall, any one transaction is not a major risk but taken together, the loss or misuse of data may have a catastrophic impact to the brand image.

The major threats in the B2C pattern are impersonation, collateral access to business systems, and misuse of personal data. Attacks based on these threats may originate from inside or outside the business. The range of countermeasures based on generic security components for a B2C pattern are: anti-virus technology, access control, authentication control, authorization control, privacy management, intrusion detection, firewalls, and encrypted transactions. These security components may be implemented OS embedded functions, special purpose security appliances, or software programs running on a business IT infrastructure.

Business-to-Business Interactions

Business-to-Business (B2B) interactions involve secure commercial transactions between one or more institutions. Typically, the transaction occurs under a contractual relationship between the parties, with either explicit or implied understanding between the parties regarding risk, mitigation and liability. The goal of the Business-to-Business pattern is to provide efficient and secure information exchange within the context of a trusted relationship.

There are three categories of Business-to-Business relationships.

Simple Supplier: one business communicates to another business for the purpose of a business transaction. The data that is being shared is not of a highly sensitive nature (for example, ordering information) so it may or may not be encrypted. Security, as an embedded attribute of B2B relationships, is employed to assure the point of entry into the business is protected from unwanted intrusion attempts or malicious code entering the corporate infrastructure.

Trusted Supplier: the sensitivity of the data increases. One example would be a hospital communicating sensitive medical data to an insurance company about a patient. During a transaction, one business may need to access data on a system belonging to another business, which may necessitate the use of authorization, access control, and auditing mechanisms.



Partnership: data now becomes shared data. In this relationship, data collaboration and sharing leads to increased security exposures in the IT infrastructure.

All of the aforementioned relationships lead to common security exposures, which can be mitigated with effective countermeasures. Generic security components that can be used to implement countermeasures include intrusion detection systems, firewalls, authorization and access control systems, along with separation of content tools. The increasing sensitivity of data in a trusted supplier and partnership may escalate the need for Virtual Private Networks (VPNs), secure e-mail and independent third party audits.

Operational Security

Operational Security encompasses the internal information technology components – software, platforms, network infrastructure, etc. – that an organization uses to execute its day-to-day business. The goal of Operational Security is to ensure that a business' internal systems and infrastructures meet required levels of security. Key drivers for operational security are geographical, regulatory and employee needs, along with tiered access to information. The core goal of this pattern is protection of brand from internal and external threats in a cost-effective manner. The critical security tools for this pattern are controlling group access, internal and external access, and data segregation.

Operational security has the following subcategories: *users, decentralized infrastructure, data centres, communications, and manufacturing*. These subcategories are differentiated on the basis of risks, threats and vulnerabilities, and then applicable mitigating factors.

Users are inside the corporate infrastructure, whether they are remote or traditional in-house desktop users. They have access to sensitive data, are typically unaware of software updates, are unskilled at security-related administration, and are often members of multiple workgroups with varied privileges that must be managed. Risks associated with users range from loss or theft of platforms/data such as notebook computers, to maliciousness such as sabotage or corporate espionage. Threats and vulnerabilities include improper configuration of personal systems, including viruses, downloadable software, and so forth. In addition, these personal systems contain a mix of personal and corporate data, as well as the opportunity for non-employee access when the system is removed from the institutions premise.



Decentralized, or “branch office”, infrastructure consists of network, server, and desktop systems that may not be directly managed by the corporate IT security staff. These systems typically manage data specific to a particular business or segment and tend to contain some aggregation of data but lack the strict controls of a data centre. The risks to these branch offices comes from unauthorized access to data, physical access to the systems, less timely system upgrades, unsecured wireless access, and poor controls on data separation and access.

Data Centres manage data of the highest value to the business (the “crown jewels”).

Typically, they are centrally managed and usually located behind additional physical and logical barriers. These systems are secured quite well and the risk of unauthorized access or modification to the data generally is small. Lack of data separation and sufficient access controls can result in catastrophic risk to the brand value by loss, exposure and misuse of competitive secrets and private data.

Communications consists of the various networking systems and related software. Risks include threats to the physical security of the network itself. The ability of the other business components to communicate effectively is based on this component. The communications systems can come under attack from external attackers who want to exploit any opportunities to gain access to the infrastructure and to disrupt the normal business operations.

Manufacturing: An optional subcategory of operational security. This is an in-house infrastructure, whether owned or leased, dedicated to the production of tangible objects.

Outsourced manufacturing is considered part of the B2B pattern. Operations may be 24 x 365, and are often connected to the business infrastructure for asset management and control. The business value of manufacturing can be extremely high since the line contains trade secrets, intellectual property and operational data. The major risk involved with this type of operational infrastructure is disruption of the line and the monetary consequences.

Physical Security: Physical security traditionally refers to “guns, guards, and gates.”

Logical security is the use of access, authorization and audit controls in conjunction with networking monitoring systems. The convergence of physical and logical security is enabled through technologies such as Radio Frequency Identification (RFID), biometric identification, and complex surveillance.



The countermeasures deployed by traditional IT security concerns, include: audit capabilities, software provisioning and version management, maintaining up-to-date anti-virus capabilities, protection of shared computing resources, intrusion detection, isolation of and recovery from security failures, as well as management of user access, authorization and identities.

High Assurance

High Assurance Systems exist where it is necessary to be confident in the security and availability of critical systems. Multiple methods can be, and usually are, used to achieve the high levels of integrity and availability of the critical systems. There is a much higher cost to achieving these levels of security, availability, and so forth, which is justified by the business value of the assets at risk. The need may arise from the sensitivity/value of the assets entrusted to an information system. The need may also arise from the consequences of a system failure.

With few exceptions, High Assurance Systems will be a small subset of a business' total set of information systems.

Examples of High Assurance Systems include national security systems, air traffic control systems, stock exchanges, and international and national banking systems. A more formal definition of a High Assurance System is:

“A system where compelling evidence is required that the system delivers its services in a manner satisfying certain critical properties.”

[Carnegie Mellon Software Engineering Institute, 2002](#)

Multiple methods can be used to achieve the required degree of integrity and availability. These include conformance testing, security evaluations, formal development methodologies, business' historical performance, and contractual methods. The specific assurance requirements and methodologies used will vary from business to business.

Some general characteristics of a High Assurance System include:

The system is secure: It can prevent unauthorized disclosure, modification, and withholding of sensitive information.

The system is real-time: It delivers results within specified time intervals.

The system is survivable: It continues to fulfil its mission in the presence of attacks, accidents or failures.

The system is fault-tolerant: It guarantees a certain quality of service despite faults, such as hardware, workload, or environmental anomalies.



The system is safe: It prevents unintended events that result in death, injury, illness, or damage to property.

The cost of failure in High Assurance Systems is much greater than the cost of failure in other systems. Failure may be measured in terms of human lives or injury to humans, loss or damage to physical systems, failure to deliver services, failure to deliver services on time, compromise of national security, and/or significant economic losses.

There are three subcategories in the overall High Assurance Systems pattern:

Enclave Environment: In an Enclave Environment, all security services are contained within a single “Trusted Computing Base.” A Trusted Computing Base, or TCB, is a tamper evident/resistant, non-bypassable collection of hardware and software that enforces a defined security policy. For accountability, communicating pairs of applications perform mutual authentication. All resources are classified for sensitivity/value. All operations on classified resources are recorded in secure logs (for example, tamper-resistant/evident). There is no network connection outside the trust boundary, so integrity and confidentiality of communicated data are not issues. However, with “trust nothing” as a root paradigm, in many cases, data will be protected in-transit and in its permanent repositories. The system may be a Multi-Level Secure (MLS) system, as defined by the TCSEC (Trusted Computing System Evaluation Criteria). The system may be evaluated under the Common Criteria (ISO/IEC 15408).

Bounded Environment: A Bounded Environment consists of multiple trusted systems (at the Enclave Environment level) linked by an isolated, trusted network. Because a network is connecting multiple trusted systems, a trusted third party may be introduced to provide mutual authentication and “over the wire” data protection (integrity and confidentiality) of the network. In addition to the assurance methodologies discussed for the Enclave Environment, this pattern introduces technology and procedures for verifying the network component, including intrusion detection systems (IDS), physical examination of the networks, and so forth.

Unbounded Environment: Unbounded Environments consist of Bounded Environments connected to public networks like the Internet, which are presumed to contain untrusted users and systems in an un-secure environment. Trusted segments of the unbounded network must defend themselves against attacks originating in untrusted segments, for example by using firewalls, antivirus utilities, cryptographic tunnels, intrusion detection/response and other mechanisms.

A business may have Bounded and Enclave Environments that remain decoupled from the untrusted network.



Business Security Patterns in action: Widgets, Inc.

In real world examples, the business security patterns should be combined to fully represent a business. The following section examines how a fictitious company, Widgets, Inc. takes advantage of many patterns to improve its business processes, work more effectively with its partners and consumers, and provides services to its employees.

Widgets, Inc is the leading supplier of widgets to the worldwide market. As shown in the figure below, Widgets has many business interactions with a variety of people and organizations to produce and deliver its product. Widgets takes advantage of the Internet to expand its business. The interactions, systems and processes create large productivity gains but these also introduce opportunities for attackers. Therefore, Widgets has implemented a secure IT infrastructure to assume leadership in the widget industry as a key provider of secure services and products. In taking this leadership position, Widgets used a combination of security patterns to manage its business risk.

In point 1 in the following figure, Widgets provides a web presence for the world to obtain access to data about the company. There is information for customers, the investor, or prospective employee. Web Presence projects a valuable image for the company. The image presented over the network is a key component of the brand image and protecting the availability and integrity of the data is important.

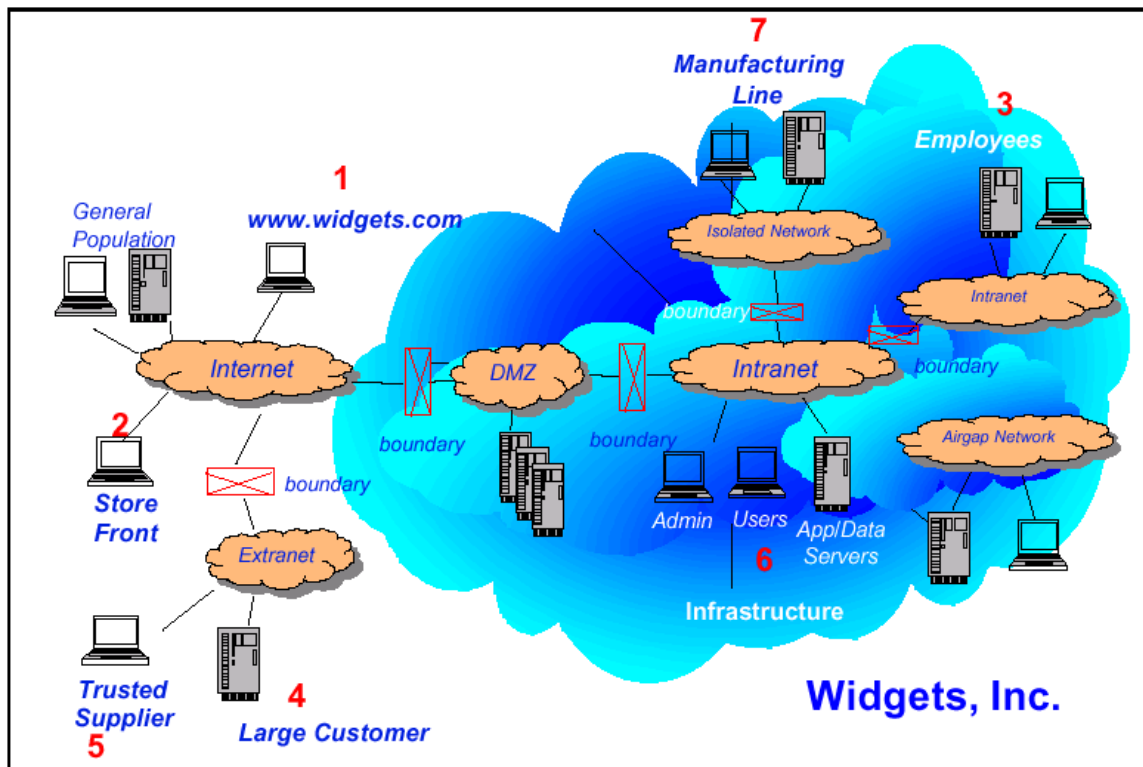
A potential customer starts interacting with Widgets at point 1, through Widgets' web presence. After evaluating the product selection and choosing particular items, the customers (virtually) moves to point 2, using a B2C business pattern. This interface is generally for small quantities of product. As part of Widgets growth plans, they see an unrealized opportunity for sales at gas stations where they can, via a kiosk (purpose optimized device) model, make ordering of widgets possible while consumers wait for their tanks to fill. Another aspect of B2C, used by Widgets in helping its employees manage their retirement accounts, medical benefits, payroll deductions and other benefits, is depicted in point 3. This is the access point for the employees. All these transactions require data protection and separation.

Widgets is the just- in-time manufacturing supplier for several large business partners. In point 4, it uses a B2B pattern to supply its product in bulk, thereby allowing closer relationships to grow by way of contracts for changes in shipping and on-demand kinds of processes. This allows Widgets to react quickly as customers' needs change. Widgets has also established, in point 5, close relationships with some of its suppliers enabling engineers to collaborate on designs and processes. Once again, securing these key business processes protects the companies and allows for close relationships to exist.



As with any company, Widgets needs to manage its internal IT infrastructure. Roughly around point 6, Widgets provides operational security for employees' machines, their access capabilities, the network, data centre, and so forth. This becomes both a competitive and productivity issue for employees. Point 7 is located on the manufacturing floor where the tightly constrained capacity requires continuous manufacturing processes. Any failure of these directly leads to irreversible revenue losses. These systems fall under much stricter controls than the normal operational systems.

Today, an implementation of High Assurance for Widgets would be cost prohibitive. However, Widgets foresees a time when higher levels of security functions will need to be deployed for mission critical systems. Widgets, Inc. employs the security patterns based on its varying business aspects. As confirmed in IBM interviews, the norm is to use a composite of security patterns to meet the total business needs of companies.





5. SECURING YOUR INSTITUTION

Understanding Patterns and your Institution

The five security patterns presented thus far represent a broad segmentation of business processes, business needs, and system elements. When applying a security pattern it is important to understand the attributes that are fundamental to a pattern as well as the associated risk characteristics. An attribute is a risk decision point. There are eight common attributes that are critical risk management decision points for key business needs, system elements and assets that require security. The specific attributes of a particular business security pattern highlight the countermeasures that a business could take to reduce risk to an acceptable level. The eight major attributes are defined as:

Who – the degree of confidence the business has in the identity of the other transacting party

Access Point – the degree of confidence the business has in the integrity of the entry point into the transaction

Access Method – the degree of confidence in the confidentiality, integrity and authenticity of the communication path between the transacting parties

Access Portal – the degree of protection the transition point provides between the trusted business and the untrusted external environment

Collateral Access – the degree to which the access to a particular resource can enable other unauthorized resource actions

Data Value – the degree of granularity required for access control to the data or the value of the data itself


Privacy – the business risks associated with maintaining and using Personally Identifiable Information and maintaining the confidentiality of other proprietary information (for example, company confidential).

Business Value – the degree to which the brand value of the business can be affected by the unauthorized unavailability, modification, disclosure or destruction of assets



The properties of the attributes change depending on the pattern under consideration. The table below qualifies the attributes on a per pattern basis.

	Who	Access Point	Access Method	Access Portal	Collateral Access	Data Value	Privacy	Business Value
High Assurance	Known by Identity	Known by Device	Ultra Secure	Protected / Locked Down	Very High	Secrecy by identity and organization	Secure	Very High: availability varies, high assurance
Operational Security	Known by Employee type	Known by Scenario	Secure / Ultra Secure	Protected	Very High	Protected & organized by owner	Organized by employee type	By Scenario: moderate availability, high assurance
B to B	Known by Contract	Known by Organization	Secure	Protected by transaction for data & business	Moderate	Protected by contract, organized by owner	Protected by contract value	Moderate / high: high availability, medium / high assurance
B to C	Self Registered Account Setup	Unknown except purpose optimized devices	Secure	Protected by transaction by data & identity	Moderate	Protected by T&Cs, organized by identity	Protected or regulated by personal value	Moderate: high availability, medium assurance
Web Presence	Unknown	Unknown	UnSecure	Protected from Write	Limited	Content Accuracy	None/ Limited	None / Limited: Limited Avail, low assurance

Center of efficiency and effectiveness 

The implementation of business security patterns will employ both technical and non-technical countermeasures (e.g. terms and conditions, contracts...etc.) based on the key risk decision points outlined in the table above. It is possible that an implementation based on business security patterns will yield effective but not efficient security countermeasures, some of which are IT resources. The attributes of *Access Portal*, *Data Value*, *Collateral Access*, and *Privacy* in particular contain multiple elements in their implementation that must interoperate within any business pattern. These elements include Web Servers, Web application servers, databases, directories, access management, messaging and collaboration software and other IT components. These elements should ideally not only interact within a business pattern, but also across multiple pattern implementations to maximize efficiency. The challenge is that each of these elements contains its own implementation of authentication, authorization, and access control that require integration.



Driving efficient integration of the authentication, authorization, and access control requires a process and enabling technology that manages the identities of users, groups and communities across all the patterns. Management of the life cycle of identities is a critical security process that is applied at all stages of an employee's or business partner's relationship with an institution. It ties together access control, authorization and authentication. It is an area where many businesses have poor or inefficient implementations. Fundamentally, identity lifecycle management assigns a user an identity with rights and privileges that will be enforced through policy. Properly implemented identity life cycle management enables systematic management of identities and related policies, ensuring uniform enforcement with and across patterns. By simplifying the user experience as well as the implementation across patterns, institutions can drive efficiency using a pattern-based approach to managing security. The IBM White Paper, *Business Security Patterns: A Methodology for Security*, elaborates further on how each pattern has different risk management characteristics as the attributes vary per pattern. The IBM White Paper, on *Business Security Patterns: A Methodology for Security*, also highlights recommended solutions for maximizing investment in the security sweet spot.

Creating an Integrated Business Security Assessment Process

Enterprises, governments and other institutions are all logically and physically built of multiple and different environments. By developing a process to understand the risk and risk management processes, these multiple different environments can be secured in a consistent, integrated, and cost-effective manner. As part of the ongoing assess, design, implement, reassess lifecycle, use of the security patterns can help determine effective risk mitigation strategies tailored to your business.

The security business patterns and associated sub-patterns provide a powerful tool for businesses. They form the cornerstone in the evaluation and implementation of a secure environment appropriate for the business being analyzed. Successful enterprise implementation of security necessitates the creation of a standard on-going process for the collection of information, evaluation, and implementation of security in a changing world of users, partners, customers, regulations and internal standards. A business can embed effective and efficient security by applying a security assessment methodology based on business security patterns that is tightly linked to the business value being delivered.

IBM Business Continuity and Recovery Services

IBM Business Continuity and Recovery Services (IBM) is a leading provider of business resilience, security, continuity and disaster recovery solutions. IBM is able to draw upon more than 35 years experience in assisting clients to develop and implement their business continuity strategies and plans. As part of this service, IBM has completed thousands of engagements, large and small, on behalf of over 5,000 clients across a range of industries around the world.



Besides its expertise in business continuity, and emergency management, IBM has skills in security, high availability solutions, systems and data management, network design and implementation, machine room building and desktop infrastructure as well as platform and application knowledge. Following its acquisition of the PricewaterhouseCoopers Consultancy, IBM also has industry-leading general business consulting skills. This ensures that IBM has a solution for any unforeseen issue likely to be encountered by its clients.

Solutions will be tailored to your multi-vendor environment, geographical location(s) and availability / risk mitigation requirements.

For more information

To learn more about IBM Business Continuity and Recovery Services in the UK, visit

[Http://www-5.ibm.com/services/uk/portfolios/bcrs.html](http://www-5.ibm.com/services/uk/portfolios/bcrs.html)

Or contact us at

E: BCRSHELP@uk.ibm.com

T: 01926 464103