Bringing it all together

Maintaining Security During an Economic Fallout

Jim Tiller
BT Vice President of Security, North America

Introduction

Enterprises worldwide are facing increasing economic uncertainty during a time when the spectrum of challenges and threats to businesses seem insurmountable. As companies brace for survival, they must make difficult decisions that will have far reaching implications on business sustainability. Many are reassessing their products and services to focus on core competencies and shedding elements of the business that do not readily align to the mission. Unfortunately for some, information security is not seen as a critical element, which couldn't be further from the truth.

Information security is more important to the survivability of businesses today than ever before. Companies have made significant investments in building their businesses and need to protect them from internal and external threats in order to maintain a strong foundation for stabilizing and ultimately rebuilding the business. Existing and emerging threats can have a profound impact with the potential to undermine even the most comprehensive reform strategies. The massive reliance on complex information technology, the inherent value of expanding information, and increasing compliance requirements have collided with aggressive and sophisticated threats from beyond and from within, representing a tangible risk to the company.

Security is the protective force that ensures corporate plans can be realized and companies can reemerge successfully as the economic environment normalizes. Organizations weakened by cuts and broad financial woes would be devastated by a successful, highly publicized attack. As companies enact their strategic plans to address today's challenges and position for long-term success, there are a number of activities that will require security to become an integral part in bringing those plans to fruition.

Interestingly, it's not about how much you spend on security, but rather the effective and innovative application of security practices that are complementary and supportive of business dynamics. It is essential that organizations embrace information security and do so in a sophisticated manner that ensures business alignment and enablement.

Today's Challenges

Around the globe, threats to businesses are manifesting themselves in a number of ways, from global economics and market forces to international competition and geopolitical dynamics. In an effort to please Wall Street, which demands demonstrable growth in any environment, companies are being forced to make fundamental changes to their business and take dramatic actions to protect the bottom-line. As cuts become deeper and deeper, remaining energy is understandably directed at revenue generation, with other parts of the business being neglected. Unfortunately for some, security has not always been seen as part of the solution in supporting business success. However, forward thinking security groups will recognize that the challenges businesses are facing today present an opportunity to engage with the business and establish a targeted approach that enables the business to move forward securely and with confidence.

Information security practices and capabilities within organizations have grown a great deal from where the security industry was a decade ago, representing the culmination of years of investments. Many organizations have gained meaningful equity through the implementation of comprehensive programs, such as information security management systems, controls frameworks, and for some, the inclusion of security metrics and reporting techniques into their programs. Yet, these well-established approaches to enterprise security typically lack one important characteristic that is indispensable in maintaining security during economic fallout: adaptability.

In tough times the ability to rapidly adapt to changes in the environment is vital to business survival and traditional security simply cannot persevere in the face of this demand. Mounting pressures on businesses to perform begin to skew perspectives of risk appetite—what may be of intense importance today may not be tomorrow. In short, business demands are a moving target and the faster information security can adapt to change, the faster it will have a purposeful and relevant influence on the business.

The lack of flexibility in existing security programs does not mean they are unable to offer any value; quite the contrary. When properly orchestrated, standard security processes can more readily enable adaptability and bring it closer to reality. Existing capabilities address the "how", but not necessarily the "how much", such as the depth and granularity of security that may be required. The key to security transformation lies in leveraging standard security processes within a services model that is inherently designed for change and tightly coupled with rapid, highly targeted risk assessments.

For example, a modified risk assessment process—which takes into consideration both business and security risks—allows for the acute application of security capabilities through a service oriented delivery model; stripping out waste, ensuring alignment with business dynamics, and through comprehensive governance, providing much needed executive level visibility into its effectiveness. The result is adaptable security; one that moves quickly to address changes, operates more efficiently and effectively, and provides usable information to ensure consistent alignment with the mission and demonstrates value.

Why Security

Economic conditions are worsening, elongating the time to recovery and reflecting an environment not equaled in the last 20 years. Since the last major recession, companies have changed significantly. Information technology is no longer ancillary; it is core to the business. The value of information has become paramount to production and is increasing in volume at a staggering rate. To effectively generate products and services, compete on a global scale, drive success, innovate, and create a comprehensive partner ecosystem, IT has become extraordinarily complex and the exchange of valuable and private information is omnipresent. In short, companies are dealing with economic stress experienced only a few times in our history and doing so in a completely different environment.

Unfortunately, today's environment is flush with threats, which are increasingly sophisticated, targeted, and evolving. Moreover, highly impactful threats are emerging from within the organization. Companies can't simply "get back to basics" because the basics do not necessarily take into account today's challenges.

For example, a predominant trend is internal threats. As unfortunate but necessary workforce reduction actions are taken, some normally law-biding people seek to express themselves by committing crimes against the company, and they find their intimate knowledge of the interworking of vast business systems afford them the opportunity to cause substantial harm.

As recently as January 2009, a contract programmer working for Fannie Mae for nearly two years reportedly planted a logic bomb upon termination that would have virtually destroyed all of the organization's 4,000 servers. Had it been successful, it would have devastated Fannie Mae and wreaked untold havoc on the fragile U.S. economy, becoming the largest known cyber-terrorism attack in history.

White-collar cybercrime is now occurring far more frequently, and verging on becoming an epidemic. Access to easy-to-use, sophisticated hacker tools is unprecedented, and in the hands of disgruntled employees with insider knowledge, their access has the potential to cause irreparable damage. Of course, this is compounded by rapidly developing external threats that are magnified in economic downturns. Companies working to implement strategic plans to stabilize the business could experience radical and unforeseen impacts deflating potential to recover successfully.

Aligning Security to Business Needs

The value of security is predominantly associated with compliance with few relating to its true value in providing business enablement. To change this mindset, security must function in a manner that is more aligned to the business' needs and produce information concerning how it is being applied in business terms that are easily digested.

Companies facing economic challenges are not entirely fearful of spending and will do so when there is clear alignment to the mission and processes are in place to ensure long-term success. What companies are demanding, and more so now than ever, is effectiveness. Not only doing more with less, but ensuring the process is fine tuned to achieve its goals economically and meaningfully.

Traditionally, security practices have been broad, basing operational integrity strictly on managing risk to the business. While this is a well-founded approach, the information resulting from these activities is not easily aligned to the corporate stability strategy. Moreover, the risk appetite of a company may change dramatically when under extreme economic pressure. In short, the environment is becoming far more dynamic, outpacing traditional risk processes. Risk management must operate more aggressively and quickly in order to address business challenges as they evolve. Therefore, a security program solely reliant on annual risk assessments, outdated threat tables, and limited visibility into the business-level risks as the only method for communicating effectiveness will experience substantial challenges. The important factor is to create agility in the existing foundation of risk management that will set in motion radical improvements to the adaptability of security and the ability to demonstrate value.

Exacerbating the situation is that security tends to be presented as an "all-or-nothing approach," which is simply not possible in today's environment. Security practices must ebb and flow with the dynamics of the business and become adjusted to apply itself in a way that is meaningful in protecting the business and doing so economically.

Understanding and Learning

Business stakeholders and the security group need to understand more intimately each other's missions and goals, as well as the metrics that define success. Historically, there has been conflict between business needs and security's desire to protect the business; where the business sees opportunity, security sees risk.

Interestingly, the impetus for change lies with the security group. For security to be effective it must completely understand the pressures business units are dealing with, what services they are responsible for and how they map to larger strategic plans, what business risks (not just security risks) they are facing, and what elements define their success. Armed with this information and knowledge, security can more accurately apply itself for the overall betterment of the company.

The first step in accomplishing this fuller understanding of the business is to review the company's mission and values. These act as guideposts for organizations as they navigate rough seas. A great deal can be garnered from monitoring how executives leverage mission and values in the decision process. This can provide visibility into key directional changes in which security can actively participate and support.

However, this is simply the beginning. Security managers need to know what the cost-cutting strategy is, and how the organization is being physically adjusted to not only accommodate reduction in resources, but to ensure long-term efficiency. Take Dell as an example. After incredible growth for several years, Q4 FY09 presented a 16% drop in revenue and a 48% drop in profits. Prior to this Dell announced a $3 billion, three-year, cost-cutting goal (later revised to $4B billion) to be met by 2011. As a result, Dell realized a more than $363 million drop in operating expense year over year. But to meet its goal, more dramatic reductions are necessary. In addition to reducing costs, Dell reorganized into four global, customer centric business units "to better meet customer and partner requirements through direct relationships, and to innovate without ties to costly, complex legacy technology."

Therefore, Dell is not only seeking to protect profitability, but changing the fundamentals of the business, which, interestingly include implications for information technology. This proves that economic times are not simply about cutting back. Companies are making fundamental changes to the operational structure of the business that have the potential to introduce additional security challenges.

It is important for security to understand the company's investment strategy and the performance metrics for those investments. Although investment generally decreases during economic downturns, spending in some areas may increase to accommodate plans and executives will have very specific expectations of returns, impacts, and timelines. It is important for security groups to be involved in helping determining potential risks and finding common ground with the business stakeholders to demonstrate applicability and value of security in meeting objectives.

Assessing a Different Risk

Managing risk is the cornerstone for security. It takes into consideration threats, weaknesses, and potential impacts to the business, providing a meaningful method for determining what controls are needed. However, in light of dramatic changes to the business and the implications of insider threats, many existing risk assessment models and processes may not be entirely effective.

Security organizations should define a risk assessment process that is modeled to reflect current company shifts, external and internal threats, and focus on specific target areas, such as business unit needs. Moreover, once the approach is refined, the assessment process must be performed quickly in order to move rapidly toward alignment. Traditionally, comprehensive risk assessments take long periods of time. However, in conditions such as these, the assessment needs to only focus on key risk attributes relating to the changes in the environment. Leveraging previous risk documentation is paramount. The goal is to adjust the model in order to incorporate new characteristics, perform a high-level assessment across the major business elements, and apply relevant data from previous assessments and audits.

The result will be a perspective of risk that provides visibility into the specific areas that represent the greatest potential for harm relative to emerging threats and business changes. Given that risk appetite has and will continue to change throughout the economic recovery lifecycle, the assessment must be rapid enough to ensure ease of repeatability, while still effective for focusing the direction of security activities.

Setting Security for Success

One of the key factors in demonstrating value and ensuring business alignment is the ability to not only apply people, process, and technology, but do so in a manner that facilitates the generation of information that speaks specifically to the overall business strategy.

There are a number of security practices that are performed regularly and may be performed in different ways. However, the details of how they are employed are not always well documented, tracked, or related to clearly articulated delivery factors. The business details of security activities do not readily surface in today's best practices, leaving the business to trust in the process. Unfortunately, trust is a rare commodity in uncertain times.

Organizing security activities into services substantially increases the ability to effectively apply resources and report in terms the business can easily digest. For example, say, based on policy, a specific security activity, such as vulnerability testing, must be performed quarterly. Historically, the activity is performed and produces a result that is used as the foundation for completeness.

Supported by a targeted risk assessment, orienting security activities into services allows the core needs of the business to be met reflecting risk appetite and recovery strategy. Revisiting the vulnerability testing example in the light of services, the policy defining when the test must be performed may be adjusted to reflect specific conditions related to a particular business unit, expectations for their systems, and the role they may be playing in the recovery process. A simple example is if an application is due for a test but that application's role—and maybe even its continued purpose—is changing, so should the testing process.

Services can define required input, ranges in service delivery, and pre-defined outputs based on business conditions and the state of the targeted environment. Security groups can start to offer levels and rates of activities relative to what is truly needed at that point in time for a given business unit. Some may interpret this as doing less, such as only addressing critical vulnerabilities, or patching specific systems, or reducing the scope of an IDS or DLP project. But in reality it is not about doing less as much as it is about surgical application of security capabilities to those areas deemed most critical to the business in light of the changing environment, and, more importantly, the direction of the business.

Attributes of service definition and early indicators of delivery methods will come from the modified risk assessment and visibility into the business strategy. Moreover, the knowledge concerning changes in threats will play a key role in their definition.

Security in the Eyes of the Business

As services are defined and structured to find a balance between traditional security activities and those needed to address localized conditions, the basis for creating greater visibility for executives is realized. This is accomplished in the following steps

- **First** - Establishing service levels for each service and creating a delivery matrix to understand the minimum conditions that are needed. This creates common understanding of expectations, demonstrates relevance to recovery strategy, employs risk assessment information, and provides the foundation for cost analysis. More importantly, when the business is inherently involved in the definition of risk and service levels, there are positive by-products, such as less time consumed in planning and justification, and greater collaboration between groups because both clearly understand what needs to be accomplished, and at what granularity. Initiation of security services becomes far more streamlined.

- **Second** - Addressing the management of the services. Defining conditions for degrees of service complexity, scope, and depth requires management of information and resources to be aligned. For example, a service may be applied to a business unit to implement configuration changes to address system stability. Under normal circumstances resources may follow an established method and execute them regardless of nuances in the intent of the project. Management provides for the ability to ensure specific methods and tools —or portions of them—are implemented relative to the service function for that particular business unit. Management activities can then be tracked and measured for performance.

- **Third** - Defining performance metrics as they relate to service delivery and to the business. These are not information security metrics, but rather indicators of performance exposing how efficient and effective a service was executed. This translates to dollars and time, as well as the use of resources. Performance metrics can express time, utilization (of people, process, and tools), quality, completeness, and management.

  The relevance to the business is enhanced through the use of services, and the ability to demonstrate effective application of those services begins to close the gap between common security approaches and business needs.

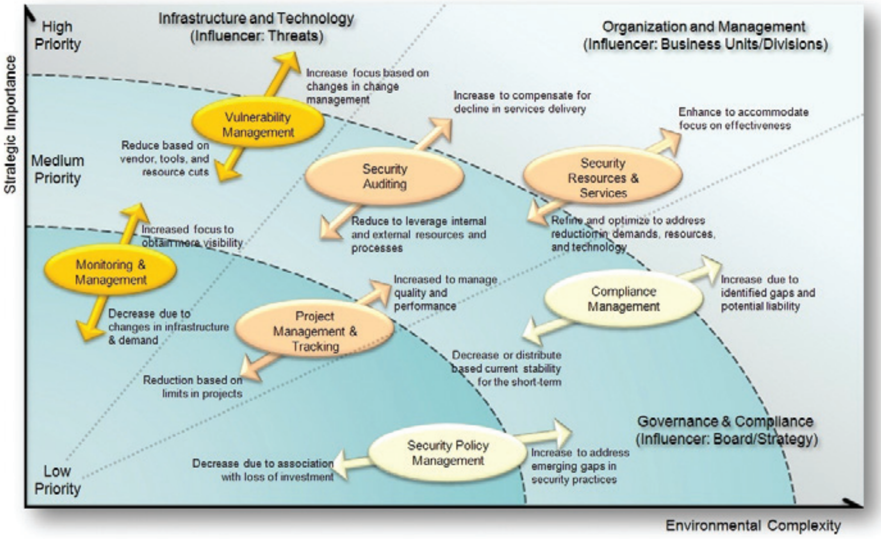
- **Fourth** - Governance of the security program as it relates to risk, business conditions, and service delivery is paramount. This simply assures that all the processes necessary to define, refine, deliver, and accurately report are working in unison and as expected. Moreover, this provides for a lessons-learned, feedback loop that ensures information from follow-on risk assessments and performance gaps in services and delivery are addressed. Governance acts as the final bonding agent between business expectations and security operations. Through governance, the identified security and business risks are translated to effective and meaningful use of resources in terms executive management can easily associate with broader directives. Ultimately, this is about the maturity of the security program and based on that maturity, security practices have the ability to be highly targeted and effective to the overall mission.

Finding a Balance

Maintaining security is important, but it also demands flexibility and accepting that not all security practices are necessary or possible. As stated previously, the all-or-nothing approach to security must be replaced with the best-impact approach to security in an environment of business needs and strategic changes.

Information security experts understand the term "compensating controls" very well. The ability to accomplish the desired level of security indirectly is commonplace. This fundamental practice needs to become the underlying force for the balancing of security services. As services are defined and implemented they will have specific criteria determining scope, depth, method, and results. By design there will be areas where there may be less security being implemented than in normal conditions. Over time, security services will allow for greater adaptability (Figure 1), ushering in the ability to dynamically apply compensating controls far more rapidly and address more accurately current business demands.

Figure 1 - Adjusting Security Services Model


Strategic Importance
High Priority
Medium Priority
Low Priority
Environmental Complexity
Infrastructure and Technology (Influencer: Threats)
Organization and Management (Influencer: Business Units/Divisions)
Governance & Compliance (Influencer: Board/Strategy)
Vulnerability Management
Increase focus based on changes in change management
Reduce based on vendor, tools, and resource cuts
Security Auditing
Increase to compensate for decline in services delivery
Reduce to leverage internal and external resources and processes
Security Resources & Services
Enhance to accommodate focus on effectiveness
Refine and optimize to address reduction in demands, resources, and technology
Monitoring & Management
Increased focus to obtain more visibility
Decrease due to changes in infrastructure & demand
Project Management & Tracking
Increased to manage quality and performance
Reduction based on limits in projects
Compliance Management
Increase due to identified gaps and potential liability
Decrease or distribute based current stability for the short-term
Security Policy Management
Increase to address emerging gaps in security practices
Decrease due to association with loss of investment

For some, when security is not applied to a particular level the business unit is typically asked to sign-off on risk acceptance. As stated earlier, risk appetite during difficult economic times is increased and if organizations are not mindful, security groups will be reduced to processing risk acceptance forms and not implementing much needed security.

When armed with a risk assessment and tracking model that reflects business and security risk, a security services framework and an underlying governance model to communicate action effectively to the business, inter-service adjustments can be made to provide for compensating controls.

For example, assume you have three security services, each focused on performing specific tasks for various business units. By definition, not all services are applied equally to all conditions and therefore each service needs to be balanced relative to risk and mission. Through a detailed analysis and consistent views from a risk perspective, undesirable condition may surface. Supplementing the risk and services model, and incorporated into the governance processes, there must exist a mechanism to connect the individual services to ensure the overall intent is achieved.

This is done through the creation of a relationship matrix that helps security practitioners and managers expose potential issues as security in one area declines. This allows for other services to be applied as compensating controls. However, this isn't simply about adding to the process. If that was the case, the services would naturally become combined and we would be right back where we started. For example, to reflect changes in delivery capability or capacity, a service may need to be reduced. As a result the relationship matrix offers a view into what other elements can be applied, such as a different service that costs less to execute and has broader delivery capacity.

Establishing a services relationship model is critical to maintaining alignment between risk and the business, accomplishing things such as:

- Ensuring that one service is not overwhelmed and consuming expensive resources, while others lie dormant.
- Taking advantage of less costly and time consuming services where applicable to better utilize resources.
- Making certain that no one service is critical to the business in light of potential future changes that might impact its delivery capacity.
- Taking advantage of strength and investments in one area to supplement other weakened areas.

This is where all the work comes together. Understanding the business strategy, building a risk model that can be repeatedly applied to view business and security risk, formulating a services model, building governance to provide valuable performance information to the business, and creating a method to ensure capabilities, investments, and processes are balanced to ensure flexibility allows for effective and efficient security to be realized in a manner that is seen as enabling the business.

Why BT

Information security is critical to business success in these uncertain times. Vast and dynamic threats have the potential to severely damage a company and undermine even the best survivability plans. However, security practices must redefine themselves and operate in a manner that enables the business to not only survive, but thrive. It's about effectiveness, flexibility and maturity in execution.

BT can help organizations realize this visionary state of cost optimization through the strategic application of our world-class portfolio of security services, uniquely delivered through our envisioning workshops. Envisioning workshops are a powerful, proven technique for exploring Business Operations issues, coupled with Technical Infrastructure positioning for true end-to-end alignment between security and needs of the business.

Envisioning workshops can quickly and cost effectively deliver a supporting framework that better prepares security services to protect a rapidly changing operational environment and frees the business to confidently focus on core products and services. Through these workshops, BT analyzes how existing standardized processes can more readily enable security adaptability, and consequently deliver the much sought after vision of a Security-Enabled Business.

Over the last several years security capabilities in many companies have become very effective at ensuring the business is protected. However, given today's broad challenges, normal operations will not suffice. BT can help security organizations raise the bar on how they interface with the business and how they provide information back into the business community to demonstrate long-term value and enable business success.

About BT

BT is one of the world's leading providers of communications solutions and services operating in 170 countries. Its principal activities include networked IT services, local national and international telecommunications services and higher-value broadband and Internet products and services. BT consists principally of four lines of business: BT Global Services, Openreach, BT Retail and BT Wholesale.

British Telecommunications (BT) is a wholly owned subsidiary of BT Group and encompasses virtually all business and assets of the BT Group. BT Group plc is listed on stock exchanges in London and New York.

For More Information

Visit **http://www.bt.com/globalservices**

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

04/20/2009