

Does Security Matter?

MAXxess Systems, Inc.
www.maxxess-systems.com

March 2006

Does Security Matter?

1.	Executive Summary	1
2.	Overview	1
3.	Background	3
	Networking	3
	Information Security	4
4.	The Changing Security Environment	5
	Strategic Interest in Security	5
	Existing Security System Environment	5
	Identity Management.....	6
	Implications for Corporate Infrastructure.....	6
5.	Today's Security Challenges	6
6.	New Expectations – New Thinking	8
7.	The EndPoint Security Management Framework	9
8.	Meeting the Expectations.....	10
9.	Summary and Conclusions – Security Does Matter	10

1. Executive Summary

Security has historically been considered a tactical, if necessary, function of most organizations. However, a large number of changes in both the nature of organizations themselves and the environment in which they operate have, over the past several years, come together to make the implementation of an effective security solution a strategic consideration for the efficient operation of the organization, its competitive position and even its very survival.

Three areas in which the pace of change is particularly rapid are: the distribution of an organization's value between physical and information assets; the scale, nature and scope of the threats to the organization; and the technology available for collecting, processing and communicating information. All of these changes have significant implications for an organization's security.

In this white paper we review key security issues and assess their impact on the organizational security function. Our overall conclusion is that this dynamic security environment is leading to significant changes in organizational responsibilities, investment priorities and the utilization of shared infrastructure. We expect these changes to continue for a considerable period of time as the expectations for security, the threat environment and the technology available for security solutions continue to evolve.

While other elements of the organization may be undergoing similar changes, security is unique not only because of its impact on the integrity – and possibly the survival – of the organization, but because of the central role that the human decision-maker plays in the security function.

How an organization responds to these security challenges over the next several years will have a significant influence on the organization's operational, financial and competitive performance. The approach to security will serve to differentiate organizations in the first decade of the 21st century.

2. Overview

In 2003, Nicholas Carr shook up the Information Technology (IT) world with an article in the Harvard Business Review (later a book) entitled *Does IT Matter?* Although worded provocatively, the question that Carr was asking wasn't "Is IT important?", but rather "Does IT serve to distinguish good companies from others?" While Carr's analysis is not without its critics, he drew a number of illuminating conclusions from this open-minded approach to the question of IT value summarized in his overall assessment that "IT doesn't matter."

Three years later we would do well to ask the same question of security. When we do so, we conclude that, unlike IT, security *does* matter. It matters not because security is intrinsically more important than IT or financial processes or any of a number of functions that today's corporations engage in; it matters because security today is in a great state of flux and those organizations that *get security right* are able to achieve and maintain a significant competitive advantage over those who do not.

In this whitepaper we will address why this is so – why security does matter and what the implication of this is. Specifically we will speak to what expectations are being placed upon the security function, how these have changed and what is likely to happen over the next several years.

Central to the conclusions we draw in this whitepaper is the observation that the security challenge has been expanding in many dimensions over the past five years and our expectation that that expansion will continue for a significant time to come. This expansion is both in the requirements for security – as a result of new threats and new vulnerabilities arising from the changing structure of organizations and changes in the environment in which they operate – and in the implementation of security – as a result of the information revolution and the commoditizing effect of shared digital infrastructure.

As a primary example, physical security and information security have developed independently in most organizations. This has typically led to separate, and very different, approaches to these two challenges. However, as an organization's value shifts between physical and information assets and as both technology and economics oblige a greater use of shared infrastructure (such as digital networks), these

Does Security Matter?

two security issues necessarily become much more interdependent. While we can see the beginning of this trend, we expect the pace of change to pick up substantially over the next few years.

The choices that organizations take to meeting these challenges are strategically important. The operational and economic consequences of these choices will serve to distinguish leading organizations and will provide competitive advantages while, at the same time, shielding the organization from an exposure to significant disruption or regulatory sanction.

While we will speak to specific technological and organizational issues, the essential conclusion of this whitepaper is that organizations today need a systematic plan for security that provides the basis for the technical, structural and investment choices necessary to establish and maintain a security environment that will meet the organization's strategic requirements.

While technology plays a critical role in this process, security remains an essentially human endeavor. Many routine tasks can, and should, be automated, but the most critical security decisions will remain the responsibility of individuals because the highly innovative nature of threats precludes a meaningful ability to predict them and, therefore, automate a response. Because of this, we believe that a powerful decision-aiding system is a critical element in any systematic security solution. We discuss one such system (The EndPoint Security Management Framework) in Section 7 as an example of how technology can leverage existing assets to address the most complex security challenges.

In summary, all organizations can benefit from a strategic review of their security needs and a measured adoption of technology to address these needs. The existing organizational security function is in an excellent position to motivate this review and to lead the process to address, and even anticipate, evolving organizational security needs.

3. Background

There is no security on this earth, there is only opportunity.
General Douglas MacArthur

The systems, the technology and the culture of security and IT have evolved independently over the past several decades. In particular, electronic security as we know it today traces its roots back to dedicated analog systems that were developed to address the need for providing cost-effective control of increasingly complex facilities by managing the growth of guard forces and dedicated security personnel. As the demands and expectations for electronic security grew, the role of corporate security management emerged from its origins within the facilities management function and began to acquire a separate identity.

Over this same time period, the corporate IT function evolved significantly as well; but in a very different manner. By the late 1960's, corporate IT was well-established as a significant functional, and cost, center within most substantial organizations. At this time, small organizations were unable to compete in the IT realm because of the prohibitive cost and expertise involved. Over the last three decades, however, IT technology developments have led to a substantial diffusion of the IT resources away from a tight central resource to a much more distributed IT environment, originally from the perspective of processing and applications, but increasingly today from a data perspective as well. While the IT organization retained a centralized purchasing and policy role, the services it provided increasingly became the networks and processes that permitted localized applications to function efficiently to meet corporate objectives. This transition actually happened in two waves; first the users moved into the network and, more recently, the storage has moved into the network.

Over the past several years, two separate drivers have begun bringing the IT and security functions of organizations closer together. The first of these is technical the second, however, represents a basic change in the security function itself.

Networking

The technical driver is the extensive use of networks – especially networks using the Internet protocol (IP) – to replace dedicated point-to-point wiring and limited bus structures such as RS-485. Much of the early use of IP networking has been for video sources (cameras and DVRs), but networking has very wide application within security systems.

Some of the current uses of IP networking for security are much like those for IT a decade ago in which capacity and conflict issues led to strict partitioning or even replication of network infrastructures. The use of IP networks for video applications, for example, is problematic since these applications typically have high bandwidth requirements and can create many issues, particularly when the networks are shared with applications other than security. IT networks today, in contrast, are widely shared, highly flexible and dynamically managed to provide not only connectivity, but guaranteed quality of service to critical users. Very few “IP-based security systems” today have been designed to participate in these managed IP networks.

IP networks are typically thought of as local structures (Local Area Networks, or LANs), but they are also becoming the dominant protocol for use in truly distributed networks (Wide Area Networks, or WANs). One of the great advantages of IP networks is that, in many ways, it doesn't matter what the network topology is; the procedure for using the network is the same. In the area of cost, however, it does matter whether one is dealing with LANs or WANs. The capacity of a network is primarily determined by its *bandwidth*. Most LANs today have a bandwidth between 100 Mb/s and 1,000 Mb/s although legacy networks may have bandwidths as low as 10 Mb/s and very high performance networks can have bandwidths of 10,000 Mb/s. The cost of this bandwidth is quite low and is typically absorbed within the overall IT infrastructure costs. In contrast, the annual cost for a 100 Mb/s IP WAN is approximately \$350,000. This cost disparity between LANs and WANs is the primary reason that most organizations provide only about 1% as much bandwidth in their WANs as they do in their LANs.

Does Security Matter?

While use of LANs for security provides meaningful operational and economic benefits, many of the greatest advantages of IP networking for security in both areas involve utilizing both LANs and WANs. Only those security solutions that manage the use of the network bandwidth, therefore, can participate in the shared IP networks that are currently controlled by the IT community. While it could be argued that, for LANs, it is possible to avoid this integration by providing dedicated IP LANs for security, this approach is not practical for the WANs. It is, therefore, critical to design IP-based security solutions for compatibility with these shared networks.

It is interesting to note that the challenge of sharing IP networks with a new, high bandwidth user is not unprecedented. In fact, the greatest growth of networks over the past decade has been the result of the migration of storage out of server platforms and into the network. In this case, the added demands upon the networks were very severe, but the economic and operational benefits were shown to be high enough to rationalize the expansion of the network requirements in order to support this new functionality. IP-based security solutions will need to address similar issues over the next five years.

Information Security

If the first driver can be characterized as the need for IT and security to live together in IT's house for economic and operational reasons, the second driver can be characterized as a growing realization that IT can no longer live without security – even if it chose to. There has been a great deal of attention focused lately on the vulnerability of IT systems because of the high concentration of information and the exposure of that information resulting from wide internal and external connectivity (brought about by the same networks discussed earlier). However, this is only one aspect of rapidly expanding need for information security.

The historical separation of physical security (that is, security for tangible assets) and information security (that is, security for intangible assets) was manageable so long as most information assets also had a corresponding physical object. Thus, for example, when customer orders came in via mail or fax the loss of corporate ERP records was an issue because of the time and effort necessary to recreate the electronic records from the hard copy (physical) records. Many companies today, however, operate in a world of electronic commerce in which transactions have no physical records; in these cases, loss of the electronic records could be disastrous.

In a recent study, the School of Information Management and Systems (SIMS) at UC Berkeley estimated that 92% of the information created by business today is *born digital*; that is, it is created and used electronically without any physical source record. Clearly, securing these information assets is not optional; it is every bit as important as securing a company's physical assets. The cost of information security has been increasing significantly over the past few years and, at the present time, as assessed by *Information Security Magazine*, averages 11% of IT spending across all organizations; ranging from nearly 20% for small IT organizations to 5% for large ones.

More recently, there has been a great deal of interest in what is being called the convergence of physical security and information security. What is meant by convergence varies widely, ranging from relatively simple incorporation of IT security monitors into physical security infrastructures to very sophisticated functions such as integrated identity management for both physical and logical access control.

Whatever its form, the growing interdependence of physical security and information security has provided the second key driver for bringing the security and IT functions closer together.

4. The Changing Security Environment

It is when we all play safe that we create a world of the utmost insecurity.

Dag Hammarskjold

Strategic Interest in Security

The security environment in commercial organizations has historically changed quite slowly. The pace of change has been limited not only by the conservative nature of most security professionals, but also by the maturity of the requirements that have been placed upon the security function itself. Additionally, security was historically seen as addressing limited tactical issues; this has led to a proliferation of a variety of point solutions (e.g. access control, fire monitoring, asset tracking) with little investment in the infrastructure that would permit an efficient integration of these functions. Over the past five years, however, security has emerged as a critical strategic issue for organizations that must be addressed much more holistically.

Traditional security systems have demonstrated the ability to meet specific security needs for many years. While it could always be argued that newer systems could provide additional functionality or could marginally improve efficiency, in most cases it was not possible to rationalize a significant capital investment based on these benefits. As an illustrative example, for a \$400,000 capital investment to exceed an Internal Rate of Return (IRR) hurdle rate of 20% (a typical level for this type of capital purchase) it would have to produce annual savings equivalent to the reduction of one full time equivalent staff position. This is a relatively high bar in environments in which requirements are not changing significantly and the primary motivation for an investment is operational efficiency.

The security environment, however, has changed drastically over the past five years. A combination of world events, technological advancement and a natural concentration of business risks have served to elevate security to the level of a strategic imperative for many organizations.

Although the security risks resulting from the necessary use of the Internet by nearly all organizations has garnered a great deal of publicity over the past few years, most security threats (even to IT systems) still come from within and effective access control and physical asset management represent the first line of defense.

One example of the challenge organizations face today is that records that once would have literally occupied buildings now are routinely stored on a single disk drive that weighs less than one pound. Various techniques are used to provide access to this data and to protect the data against the failure of the disks, but these techniques invariably have the effect of producing multiple copies of the records distributed throughout the organization. Providing security for these multiple copies of critical data has proven to be a major challenge and this security is a major issue not just for operational management, but executive management and company directors as well.

Existing Security System Environment

Most security environments have evolved over a considerable period of time and use. They therefore represent a significant investment in both capital assets, training and operational experience. While many of these systems do not represent the optimal solution to today's security challenges, they typically meet traditional security needs. Due to the time periods over which these systems were implemented, particularly within distributed organizations, they typically represent a collection of point solutions to site-specific requirements (access control, monitoring, etc.). The technologies in the systems have not been amenable to combining these individual systems into an integrated solution as, for example, as has typically been done with isolated IT systems, for either functional consolidation or operational efficiency.

Identity Management

From a security perspective, Identity Management (IM) has been an access control function that often reflects significant site-specific characteristics. Over the past decade, leading access control systems have incorporated highly integrated interactions with other personnel management systems (such as Human Relations databases) to IM in an efficient and effective manner. Over the same time period, IT systems have developed a, limited form of IM to control access to various elements of the information infrastructure. These two components of IM have historically not been integrated.

At the present time there are two important drivers that are obliging organizations to seriously address the integration of these separate aspects of IM. The first has already been discussed under *Background*: since the value of information assets in organizations far exceeds the value of physical assets, management has begun to demand the same degree of advanced management for information identity management that it has for physical identity management. The second driver for the integration of IM, at least in the US is HSPD-12 (Homeland Security Presidential Directive 12), which requires a comprehensive IM implementation with substantially new requirements for both physical and information identity management. This directive calls for an implementation by late 2006 by many agencies of the federal government and by those organizations dealing with these agencies.

By most accounts, IM is going to be the area in which the most significant new requirements for physical security are going to arise over the next few years.

Implications for Corporate Infrastructure

The location of the security function in most organizational structures reflects the tactical attitude that these organizations have had toward security. Security, however, has emerged as a strategic threat to organizations over the past five years. The level of expectation for security implementation has increased significantly and many organizations have elevated the executive security responsibility to a Chief Security Officer (CSO) who operates at parity with the COO, the CIO and the CFO. It is important to note that, while security is often characterized as the management and response to external threats, a recent survey by TheInfoPro™ found that 72% of corporate decision-makers considered that internal threats posed a greater challenge to the organization than did external threats.

At the same time, cost-effective implementation of new, highly consolidated security solutions will require that these solutions share corporate infrastructure with other critical functions such as IT. It is no longer a question of whether or not security can take advantage of resources such as networks, managed storage and communications nominally managed by other organizational functions, but rather where the optimal allocation of these resources should be from both an operational and a financial perspective.

5. Today's Security Challenges

As a rule, he or she who has the most information will have the greatest success in life.

Benjamin Disraeli

Security managers today, therefore, face a challenge shaped by a number of dynamics: some internal to the organization and others external; some reflective of the technical environment of the organization and others reflective of the security environment; some driven by organizational changes and a shift of resources or responsibilities; some representative of the growing recognition of the criticality of protecting information assets in a manner more consistent to that used for physical assets; but all driven by an overarching economic pressure to make most effective utilization of corporate infrastructure assets and to minimize on-going operational costs. At the same time, the recognition of security as a strategic requirement for the organization brings with it an expectation of greater functionality and flexibility than had previously been the case.

While it could be argued that this type of change applies to all significant organizational functions and not just security, the critical operational nature of security presents some unique aspects of the strategy necessary to accommodate the organizational and requirements changes. In particular, some of the

Does Security Matter?

changes arising from new technological options can make the core security challenge more – rather than less – difficult.

As one example, consider the ubiquity of video and, in particular, networked video (often called, inaccurately, “IP surveillance”). While it may appear obvious that the addition of high quality video significantly aids the process of security decision making, this is strictly only true in an environment free of constraints on critical resources such as bandwidth and human attention. In many practical situations, the addition of video can reduce the quality of service for other users of shared networks (including other security users) and distract, rather than enhance, the time-critical decision process. The issue isn’t whether IP video is *good* or *bad* for security but rather that the manner in which this technology is integrated into a security solution will have a dominant impact on its ultimate utility.

Video, in fact, is an example of a larger trend that security system architects face. With the profusion of digital networks and the economic imperative toward not only digital, but networked digital sensing, the amount of data that can be presented to the security decision maker in real time has expanded tremendously – to the point of saturating, and even overwhelming, the ultimately critical element – the human element – in the system. When viewed from a human factors perspective, there are two critical issues that must be addressed: the *needle in a haystack* issue and the *tunnel vision* issue.

The *needle in a haystack* issue comes from the fact that most of the time security sensors provide data that has very little important information. They occasionally provide data that has very important information but, unless it can be characterized to the security decision maker as such, it can easily be ignored or lost. This issue, of course, has been an element of security management for a considerable period of time, but the growth of cost-effective sensing technologies has tremendously increased the scale of the issue.

The *tunnel vision* issue arises from the scope of the security challenge. Effective resolution of security events often requires detailed analysis of very specific systems and records; at the same time, the response to an event must be made with full awareness of the context in which the event occurs. If the process of detailed analysis of events obliges the security decision maker to lose the context of the *big picture* context, those decisions will be at best sub-optimal and at worst invalid or ineffective.

One dimension of today’s security challenge remains unchanged; the need to make and implement critical, often unstructured, decisions in real time. Security analytics, therefore, are different from the analytics of other functional areas in the organization in that the timeliness of the decisions is of paramount importance. Technology has enabled us to increase the amount of data available for making these decisions and has increased the speed with which that data is collected, communicated and processed – up to the final stage of the process which is necessarily human decision-making. Unless we are prepared to utilize the available technology to enhance the effectiveness of this last step, we will have very little impact on the quality of the resulting decisions.

In summary, we are placing much higher expectations on security in terms of both scale and scope. Security has new tools and technologies to support its implementation and, in many cases, the effective uses of those technologies require a much higher level of integration between security and other functional areas of the organization. The need to respond to new threats – both real and perceived – has led to a rate of change in requirements for security that is much higher than we have historically seen and, finally, we expect security to respond to all of these challenges in an environment in which the economic implications of the solution will be examined much more strategically than has been done in the past.

6. New Expectations – New Thinking

A problem can't be solved with the same thinking that created it.
Albert Einstein

Most of today's security solutions were designed to solve a problem that was qualitatively different from the one faced today. It requires new thinking to effectively address today's security challenge.

The first aspect of the new thinking is a recognition that the security challenge today consists of an intimate blend of three elements. While the specifics will vary from organization to organization, the three primary elements for security are information management, real-time decision making and implementing a response based upon the decision. All three of these elements must be considered in order to implement a security function that will meet both today's expectations and the emerging requirements for both enhanced functionality and greater operational efficiency. It is therefore essential to assess the implementations of technologies such as IP surveillance within the context of the whole security challenge to make conscientious investment decisions for security.

The second aspect of the new thinking is the relationship between security and the rest of the organizational infrastructure. Where it was once considered acceptable, even desirable, for security to be implemented as a standalone function, both the pervasive nature of the security challenge and the resources required to accommodate the real time delivery of the information required to make effective security decisions oblige a high level of integration with major organizational infrastructure. This integration with organizational infrastructure and other functional areas, of course, brings with it the risk of deleterious interactions – both on a technical and on an organizational level. These issues must be anticipated and managed on a pro-active basis in order to meet the operational and fiscal requirements of the organization. The cost of organizational turf battles is high; the result of attempting to avoid the integration challenges is highly sub-optimal implementations with both performance constraints and economic penalties. The leadership for this integration process may come from the CEO, the CFO, the CSO or the CIO but, in any case, it must have corporate-wide support to implement the necessary technical, operational and cultural change.

The final aspect of the new thinking is a recognition that the security challenge is to implement a process that can accommodate evolving security requirements and capabilities over a considerable period of time. Since the threat model is neither completely known nor static, security solutions need to be flexible enough to respond to both quantitative and qualitative changes in both requirements and expectations. Additionally, the continued development of an organization's technical infrastructure means that objectives that cannot be technically or economically addressed today may become very practical as the supporting infrastructure evolves. As one example, wide area connectivity at ¼ T-1 bandwidth (roughly 350KB/s) was only economically viable for large facilities five years ago; today with DSL technology, this bandwidth is practical for even the smallest of facilities.

These three aspects can be summarized as:

- Consider the whole security challenge,
- Understand all of the implications of integration with the organizational infrastructure, and
- Recognize that the solution must evolve to adapt to changing requirements and environments.

7. The EndPoint Security Management Framework

Over the past several years, MAXxess has focused on analyzing the organizational security challenge in the context of emerging technologies, evolving corporate economics, new expectations for security and the new thinking on the approach to addressing this challenge. As a result of this analysis, MAXxess undertook the development of a security management solution that was responsive to both the evolving security challenges and the technical infrastructure available in a wide range of security environments. We called the new solution EndPoint to emphasize its role at the nexus of information, decisions and actions related to security.

The primary objectives of the EndPoint development were:

- Integration of traditional security and other data sources at the information level to minimize the complexity of accommodating a wide range of data sources from legacy security, fire detection and building management systems to information infrastructure systems such as ERP, CRM and IT security monitors
- Organic use of IP infrastructure, including LANs, WANs, organizational intranets as well as the Internet, not just for data transport, but as a source of contextual information
- Consistent, structured, virtualized, visual presentation of all information that is compatible with hierarchical management structures and that can be tuned to enhance human decision-making and minimize cross-training requirements
- Preservation of critical contextual information (situational awareness) from the highest to the lowest operating level of the system
- Distributed processing and information management architecture that permits affordable centralization of critical security management functions while minimizing bandwidth costs
- Ability to control, not just monitor, critical systems in response to events
- Capability to scale and adapt to accommodate evolving organizational structures
- Compatibility with redundant management, computation and communication architectures.

Equally important, the EndPoint development was focused upon producing a practical solution for a very broad range of organizations so the implementation costs needed to be minimized by:

- A standardized, replicable software structure that can be configured, rather than redesigned, to meet unique organizational requirements
- Modularization of critical functionality and the ability to scale an existing implementation with little or no operational interruption so that configurations can be tightly tuned to immediate organizational requirements
- The ability to utilize standard Windows-based platforms for all computing requirements
- A minimization of the operational bandwidth requirements to accommodate distributed resources

The resulting solution, the EndPoint Security Management Framework, was introduced late in 2005 with its first operational installations implemented early in 2006. As might be expected, these early implementations have focused on the integration of traditional security (primarily, access control) systems with limited integration of auxiliary information sources. As these solutions evolve, we anticipate that they will expand their use of information sources external to the traditional security space to meet more sophisticated security requirements.

Most of the early EndPoint implementations are providing centralized management of a distributed security environment. While this need not necessarily be the case, the economic benefits of EndPoint are strongest in these distributed environments.

The purpose of this white paper is not to describe EndPoint in detail, but rather to use the EndPoint example to illustrate the characteristics of solutions that can effectively address today's complex security challenges. Further information on EndPoint can be found at www.maxxess-systems.com.

8. Meeting the Expectations

It is not necessary to change. Survival is not mandatory.
W. Edwards Deming

Many organizations have demanding new expectations for security. These expectations are driven by real business imperatives and operational necessities and have become a critical element in the strategy of the organization. There are, in many cases, technological approaches available to meet these expectations, but a systematic solution environment is required to both address these expectations in an economically viable manner and to accommodate the continued evolution and growth of these expectations over the next several years.

The necessary changes are often as much organizational as they are technical. At the present time, it is rare for one function to have cognizance of the entire set of security requirements for the organization; for example, in most organizations the responsibilities for physical security and information security are currently split between the security function and the IT function. While it is clearly possible to extend the segmentation of security responsibilities to meet new requirements, the need for economic efficiency will drive a trend toward more integrated solutions. The home for these integrated solutions can either be within the IT function (which currently has control of much of the necessary technical infrastructure and some of the security budget) or the security function (which currently has the security mission, has control of major dedicated security systems and has some of the security budget). The organizational choice will often reflect the relative strength of leadership between these functions. In any case, the function that steps up to the new security challenge will necessarily impose on the charter of other functions in the organization.

While organizations will rationally strive toward meeting their new security expectations while minimizing both economic and organizational costs, the strategic nature of the security challenge ensures that they will accommodate those changes that are necessary to meet these challenges.

Executives that are currently charged with the organizational security function are in an excellent position to lead the change process necessary to enable the organization to meet its new challenges in this area. The extension of the security function into new operational and infrastructure areas is an unavoidable consequence of the need to address these challenges in a coherent and integrated manner. Alternatively, it is possible for other functional areas to step up to the integrated security function. In this case, however, it is critical that these functional areas adopt the full mission and culture of the security responsibility, not just the technical solution.

9. Summary and Conclusions – Security Does Matter

In summary, we come to the conclusion that, unlike Nicholas Carr's assessment of IT, security *does* matter. It matters in the sense that an effective approach to meeting new security expectations will serve to differentiate organizations in the market over the next several years. Those organizations that do not step up to the new security challenges will place themselves at risk and will be exposed to the very real threat of the loss of significant assets (tangible or informational) or disruption or loss of operational functionality for a significant period of time which, in many industries, can be even more damaging. It also matters in the sense that the economic implications of how these challenges are met are significant enough to impact the organization's competitive position in the market.

Technology is becoming available that will enable organizations to address new and emerging security requirements in a rational, affordable manner. In considering these technologies, however, it is critical to keep in mind that in security solutions, the major criterion for assessing these technologies is the degree to which they support the most critical and the most expensive component of the overall security function – the human decision-maker.