IBM security solutions
White paper

IBM Security Technology Outlook: An outlook on emerging security technology trends.

October 2008

Contents

Executive summary

In the next two to five years, emerging technological and social trends will have far-reaching implications for enterprise security. This white paper outlines the fundamental technology trends organizations can expect to see in the next several years, the catalysts behind those trends and the ways in which IBM can help organizations strategically balance risk with opportunity.

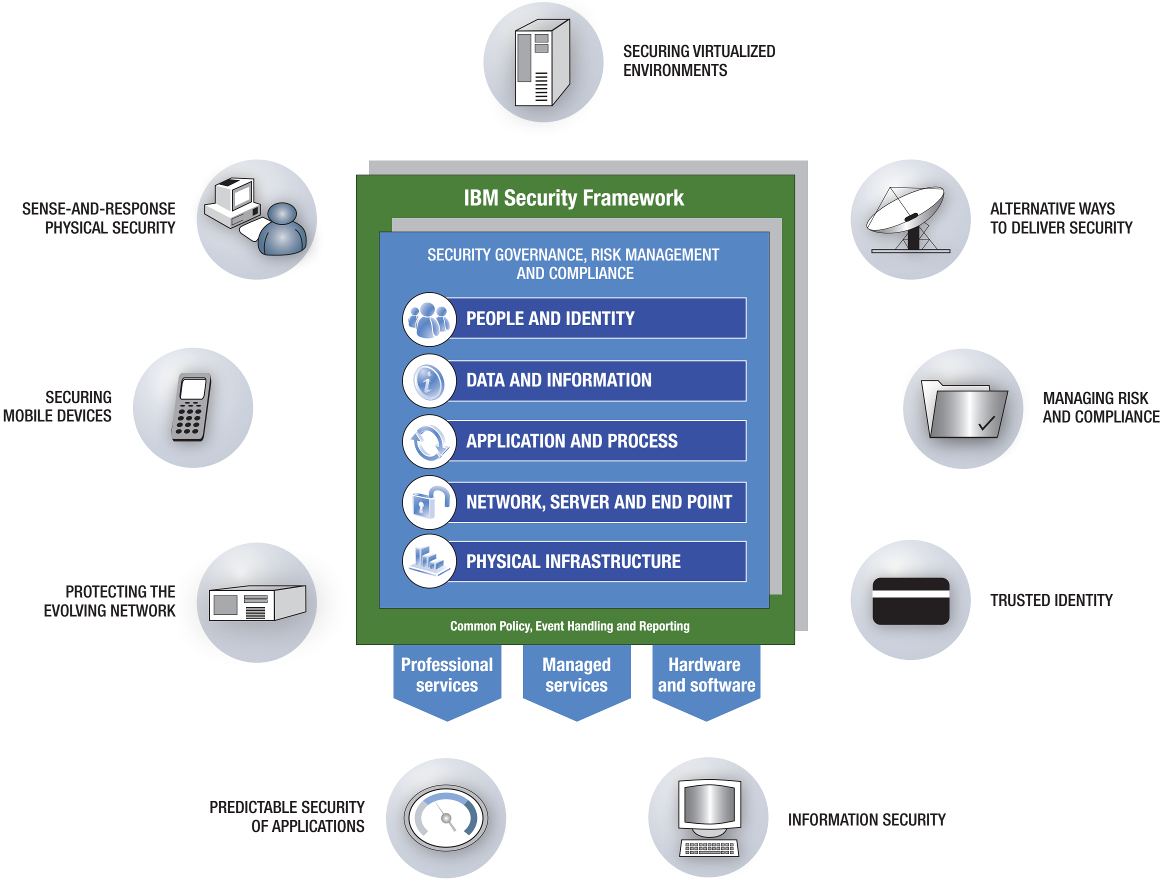
Introduction

As the pace of globalization picks up, traditional boundaries continue to disappear, melting before the relentless pace of 24x7 communications and trade. In this new global reality, “open for business” can mean pooling resources and sharing sensitive information among organizations are the de facto costs of admission to the global economy.

The line between participation and isolation can also mark the line of opportunity and risk. Now more than ever, we rely on our business systems and automated policies to guard that line – to root out the threats, to safeguard our intellectual property, to protect our reputations and privacy.

With the emergence of each new technology, the line can shift just a bit. As we rush to exploit the opportunities, determined insiders and outsiders may seek to exploit vulnerabilities. Consequently, the potential of emerging technologies marks a fundamental change in how organizations should approach the accompanying security challenges.

To gain a perspective on the security challenges organizations will face in the next several years, the following questions should be considered: What fundamental technology trends are expected to impact organizations in the next two to five years? What strategic drivers should serve as catalysts for change? And how can organizations position themselves to profit from the myriad opportunities while managing the risk that inevitably accompanies them?


SECURING VIRTUALIZED ENVIRONMENTS
SENSE-AND-RESPONSE PHYSICAL SECURITY
ALTERNATIVE WAYS TO DELIVER SECURITY
SECURING MOBILE DEVICES
MANAGING RISK AND COMPLIANCE
PROTECTING THE EVOLVING NETWORK
TRUSTED IDENTITY
IBM Security Framework
SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE
PEOPLE AND IDENTITY
DATA AND INFORMATION
APPLICATION AND PROCESS
NETWORK, SERVER AND END POINT
PHYSICAL INFRASTRUCTURE
Common Policy, Event Handling and Reporting
Professional services
Managed services
Hardware and software
PREDICTABLE SECURITY OF APPLICATIONS
INFORMATION SECURITY

We began this conversation with the Global Technology Outlook (GTO) and the Global Innovation Outlook™ (GIO) in which we shared insights around the most pressing security problems, among others. During the course of hundreds of customer engagements and extensive market research, we've continued to think forward with the end goal of turning these insights into actions organizations can take now to prepare for the opportunities ahead. Our collected analysis therefore points to nine important trends and technologies that are expected to shape the security environment in the next two to five years. These include:

In the next few years, security requirements are expected to be driven by:

- A highly dynamic IT environment that can respond efficiently to elastic scalability demands.
- The ability to use electronic identities for sensitive and mission-critical purposes.
- End-user demands for more control and self-determination with their online identities.
- Secure, reliable, flexible and composable applications that can facilitate a rapid response to changing business needs.
- Accommodation of the organization's desired level of control of the IT environment.
- A risk-based approach to managing IT security and its contribution to operational and business risk.
- Mobile devices to be a secure source of identity and a business platform.
- High-risk decisions based on secure, high-quality information sources.
- IT systems that can sense and respond to the real-world environment.

- *Securing Virtualized Environments* — From dedicated hardware for dedicated purposes to shared hardware for dedicated applications.
- *Alternative Ways to Deliver Security* — Prepackaged security for easy deployment and quick time to value.
- *Managing Risk and Compliance* — Business risk–based and policy-driven approach to managing IT security.
- *Trusted Identity* — Toward trusted, privacy-enabling, shared and easy-to-use identities.
- *Information Security* — Reflecting the business value of data at risk.
- *Predictable Security of Applications* — Integrated security throughout the application lifecycle.
- *Protecting the Evolving Network* — Real-time security regardless of network speed, with protection against the rise in application-specific attacks.
- *Securing Mobile Devices* — A trusted channel for conducting business and a primary means for authentication.
- *Sense-and-Response Physical Security* — Efficient and decisive physical security.

These trends frame our discussion of how organizations can respond to the security challenges of the emerging technological and social changes ahead. In the following sections, this paper will outline what those technologies mean, the potential that comes with them and the ways in which IBM can help organizations strategically manage the challenges, risks and opportunities ahead.

IBM and the security landscape

Over the last several years, the evolution from the physical to the digital world has transformed the security landscape. Survey data collected by IBM shows that as more sensitive information has moved online, highly coordinated attacks against individuals and organizations have become both more frequent and sophisticated with each passing year. The targets themselves have expanded – in the future, smart phones, payment systems such as radio frequency identification (RFID) and "Chip and PIN" systems, and even home entertainment systems may be progressively more vulnerable.

Increasingly aware of the risk to their personal identity and information, individuals are demanding that organizations take the necessary steps to safeguard it. These expectations are reinforced through laws and regulations created to protect the privacy of personally identifiable information – credit card numbers, medical records and other potential targets. Organizations in turn should protect their own intellectual property and reputations from catastrophic breaches.

These changes and challenges in the technology environment have helped shape IBM's own approach to security. Designed to help organizations strategically manage risk across all areas of the organization, the IBM Security Framework identifies five key security areas or domains, including people and identity; data and information; application and process; network, server and end point; and physical infrastructure. By examining each of these domains in the context of potential risk elements and impact, organizations can better understand and prioritize risks and vulnerabilities.

IBM intends to continue to build on the momentum we've created with our security framework through new offerings and services that tackle the increasing sophistication and diverse nature of security requirements, and in doing so, enable organizations to confidently realize the benefits these trends will bring.

“Information systems labor costs can now represent up to 70% of an information technology (IT) operations budget; power and cooling costs are now 8x greater than a dozen years ago.”

— Clabby Analytics[1]

Looking ahead

Since it first introduced virtualization IBM has continued to define and redefine virtualization technologies on its System z® and System p® platforms. The IBM z/VM® system, for example, can run thousands of fully isolated Linux® systems simultaneously. As virtualization accelerates beyond the mainframe, IBM is applying the knowledge gained over the decades to other virtualization platforms.

IBM continues to research and develop technologies for managing the security of virtualized environments through its Phantom project for virtual machine (VM) protection and secure cross-VM communication, and for managing full infrastructure isolation through its Trusted Virtual Domains research project.

As part of its ongoing commitment to stronger security within virtualized environments, IBM Internet Security Systems (ISS) Proventia® offerings have been extended to virtual form factors, IBM Tivoli® Access Manager for Operating Systems is providing capabilities to monitor privileged user activity in VMs, and IBM WebSphere® DataPower® SOA Appliances provide security protection to applications running on virtual hosts.

In addition, the IBM Blue Cloud offering helps operational center services run across a distributed, globally accessible fabric of resources, rather than on local machines or remote server farms.

Trend 1: Securing Virtualized Environments

For the past two decades, organizations have raced to keep up with changing technology requirements by substantially building out data centers. With operational centers already stretching the upper limits of power, space and staff resources, soaring capital costs and exponential growth in power costs are forcing organizations to examine ways to deliver a more energy-efficient infrastructure.

Unprecedented levels of scalability and responsiveness should also be in place to support the dramatic growth of shared applications, and the natural ebb and flow of service demands on resources. Based on a shared infrastructure in which large virtualized resource pools are linked to provide organizations with a simple, quick and device-agnostic path to services, cloud computing delivers the potential to radically change the economics of running a data center.

Through the ability to define and standardize collections of resources, cloud computing offers simplification on a grand scale, providing an opportunity to streamline and standardize the security approach and configurations throughout the organization. In turn, the simplification feeds on itself – since resources can be managed in a similar fashion, a larger number of virtual resources are manageable.

Despite the tremendous opportunities cloud computing holds, however, it can also bring additional challenges:

- Organizations should be prepared with strong isolation management capabilities that separate the applications, data and infrastructure dedicated to one tenant from the rest of the tenants, with isolation policies that can be applied across multiple virtualization platforms.
- The integrity of the virtual environment should be protected and managed as robustly as the physical environment. Traditional security capabilities, such as network monitoring and intrusion detection, should be applied to the virtual environments.
- Because virtualized resources are stored as data images, they are subject to corruption. Organizations should establish image management capabilities to protect and maintain the resource definitions, including robust change and patch management procedures.

Trend 2: Alternative Ways to Deliver Security

The economics of managing and operating complex, specialized IT security services is driving a focus for new forms of packaging and delivering security services. There are two key factors that influence this increased diversity.

First, the IT organization should decide how much control they want to maintain. Are they comfortable with the idea of another company providing their security services or do they want to manage security themselves?

Second, the complexity of the IT environment can heavily influence how the IT organization chooses to obtain security capabilities. Some companies have relatively simple, self-contained IT needs. On the other hand, some companies have highly dynamic environments that have the ability to quickly adapt their IT services to new business needs.

In addition to traditional software offerings, managed services and outsourcing arrangements, IBM sees several trends in the delivery of security capabilities:

Appliances. In the past, IT appliances meant "one host dedicated to one specialized function." Today's appliances are becoming platforms in their own right, evolving to a single deliverable that contains all of the operating system, middleware and applications preinstalled and preconfigured to perform multiple functions targeted to a single domain of operation. Appliances are also moving to increasingly modular physical form factors as well as virtual form factors.

Software-as-a-Service (SaaS). While managed services typically have dedicated infrastructure for each customer, SaaS platforms deliver "one-to-many" service in which a single platform provides a type of service to multiple customers simultaneously. These shared infrastructure systems can provide standardized services with little need for customization.

Cloud computing. Virtualized platforms and cloud computing environments support highly dynamic environments with elastic scalability needs. These dynamic environments can be used to create "cookie-cutter" definitions of resource pools to standardize application deployment and other IT services that can be deployed in massive numbers in very short times, leading to a "utility" approach to consuming security services.

Looking ahead

IBM is an industry-leading provider of services and solutions helping IT organizations analyze and understand their operational risk. When the banking industry formed the Operational Risk Exchange to share operational risk data with each other and establish industry benchmarks, IBM brought the analytics expertise. IBM Banking Data Warehouse provides a proven model for managing operational risk. IBM Cognos Risk Management Cockpit, along with the other products in the IBM Cognos Business Intelligence solutions family, provides risk reports, dashboards, event management, scorecards and risk analysis capability in a single environment.

The IBM service oriented architecture (SOA) policy management strategy provides a traceable way to associate security policies with SOA services and transform those policies into security requirements and security configurations.

For managing security configurations, IBM Service Management offerings and the IBM Tivoli zSecure family of offerings enforces rigorous change control processes on IT environments, while IBM Tivoli Compliance Insight Manger, IBM Tivoli Security Compliance Manager and IBM Tivoli Security Information and Event Manager monitor for out-of-process security issues.

Trend 3: Managing Risk and Compliance

Many organizations are re-examining their business continuity and resiliency strategies. Companies are realizing that disaster recovery plans are simply not enough; even everyday small disasters can have big consequences for a company's ability to conduct business.

Operational risk can cover any activity that impacts business processes, including theft, insider fraud, loss of physical facilities or other capital assets, and failure to meet safety and other regulatory requirements. Because IT is ingrained in virtually every aspect of a company's activities, IT risks are a major component of operational risk. For example, what if an unauthorized employee is able to bypass the security protections of a key financial reporting application? What if archive tapes with customer data are lost? What if the data center loses power? Looking at IT security and resiliency issues from an operational risk perspective helps the chief information security officer (CISO) prioritize time and money investments in ways that can have the best impact on the company's operations.

However, more and more of the IT landscape is out of the direct control of the CISO – through outsourcing, IT integration with business partners, the use of managed security services or other IT resources owned by others – which means the CISO is becoming an increasingly policy-driven and consultative job. IT security is therefore evolving toward evaluating IT's contribution to operational risk and developing policies and controls to mitigate those risks both in the IT infrastructure controlled by the CISO as well as outside IT resources.

"Our identities are under attack from all sides, with identity theft claiming a new victim about every 2 seconds."

— Facts and Statistics, Identity Theft Resource Center, April 30, 2007

Trend 4: Trusted Identity

In a global economy where billions of people connect daily, identity has taken on a new focus. Each transaction depends on the level of trust each party places in the integrity of the other's credentials and the systems supporting them. Yet considering the rising instances of identity theft and fraud, that trust may well prove overly optimistic.

With the goals of improving identification and enabling higher-value transactions – like healthcare authorizations and high-value banking operations – governments and enterprises are working to create identity management models where baseline identities can be more highly assured, with stronger identity credentials that are better protected from tampering and forgery.

On the commercial side, identity systems continue to proliferate, forcing individuals to become their own identity administrators, juggling a mixture of self-created and third-party issued identities for every service they interact with, and balancing the trade-offs between privacy and reputation that come with increased disclosure.

Going forward, the challenge lies in developing a common set of identity policies, processes, best practices and technology, as well as multipurpose identity systems that can be used across service providers. These systems should be able to accommodate complex identity relationships while providing a simplified way to address common identity processes and functions, including enrollment and proofing, credential management and identity usage. At the same time, the identity systems should respect the corresponding conventions and limitations of societal and cultural boundaries, including privacy, reputation and individual rights.

Looking ahead

Building on IBM's industry-leading Tivoli Identity and Access Management family of products, as well as the Tivoli zSecure suite and IBM Resource Access Control Facility (RACF®), IBM is finding solid and sustainable solutions to present and future challenges.[2] IBM is working with open standards organizations to make identity management simpler for individuals. IBM is a major contributor to the Eclipse project Higgins, which defines a user-centric "identity metasystem" to give individuals more control over their credentials and personal information. IBM is also a supporter of the OpenID initiative, an open-standard, third-party credential provider that enables individuals to use a single credential across multiple online services. Both of these systems are supported in IBM Tivoli Federated Identity Manager.

The IBM Trusted Identity initiative tackles the weak links and end-to-end integration problems in current trusted identity systems, ranging from the identity proofing stage — where a large percentage of identity fraud and theft has its roots — to the usage of trusted identities in online and offline scenarios.

The trusted identity showcase — a focal point for state-of-the-art identity management technology — offers demonstrations and executive briefings on improving identity proofing using IBM Global Name Recognition and IBM Relationship Resolution technologies.

According to the Privacy Rights Clearinghouse, over 226 million records containing sensitive personal information have been involved in security breaches since they started counting in 2005.[3]

Looking ahead

IBM is a leader in hardware-based encryption management, offering a line of encrypting tape drives such as the TS1120 and TS1130, and full disk encryption capabilities in the IBM System Storage™ DS8000 Series family of disk systems, including file system-level encryption capabilities for IBM DB2® servers. IBM also offers an enterprise-scale key management infrastructure through IBM Tivoli Key Lifecycle Manager and lifecycle management tools to help organizations efficiently deploy, back up, restore and delete keys and certificates in a secure and consistent fashion.

DB2 and IBM Informix® offer access control features including a sophisticated Label Based Access Control (LBAC) mechanism that allows administrators to control read and write access of a user at the table, column and row levels. DB2 and Informix also support single sign-on through Kerberos integration.

As part of an integrated data management approach, the IBM Optim™ Data Privacy Solution provides policy-based deidentification and masking capabilities to protect confidential data, while the IBM Optim Data Growth Solution helps enforce secure access to archived data based on established data governance policies.

These data protection capabilities provide a trustworthy foundation to use enterprise information assets for business optimization in a way that reflects the value of information and protects individuals' privacy. The IBM InfoSphere™ and IBM Cognos product families build on the security foundations to ensure that information is accurate, complete, in context and actionable.

Trend 5: Information Security

Today, an ever-expanding volume of information continually and freely circulates across and beyond enterprises, governments and social networks, aided through the proliferation of open, collaborative environments, Web 2.0 mashup technologies and intelligent data streams. A boon to online communities, the information explosion has nevertheless created a nightmare for organizations with the proliferation of databases and corresponding increase in data leakage that raises the potential for data breaches and the chance of inappropriate disclosure or use of intellectual capital.

Already a boardroom issue, organizations can expect a continued push to minimize the risks of data breaches. As a result, there should be a new focus on privacy management tools with the capability to mask data, particularly in nonproduction environments such as application development where protection of data continues to be less stringent. This focus can reinforce the need for cryptography, and subsequent demand to simplify the complexity of the key-based algorithms and management of keys throughout the lifecycle.

There is expected to be more internal pressure to link trust in data with decision making. Collectively, security practices – including data steward assignments, data monitoring, policy-based data classification and security requirements records – should provide the metrics that calculate and reflect the security protections for a particular repository. These metrics can be used in formulating "trust indexes" that can guide decisions about the use of a data repository – a repository with a high trust index association can be used for high-risk decisions; conversely, a repository with a low trust index association should be used only for low-risk activities.

Trend 6: Predictable Security of Applications

In 2008, a new type of threat known as SEO code injection or poisoning impacted around 1.2 million Web sites, including some very high-profile sites. As the dust settled from this exceptionally destructive threat, it became clear that applications had become ground zero for hacker attacks.

Part of their vulnerability lies in the evolution from monolithic applications to composite applications, both in SOA–style process choreography and through Web 2.0–style widgets and mashups. These composite applications can include application code from a wide variety of sources in a true mix-and-match fashion. Though it has tremendously improved programmer efficiency and enabled many nonprogrammers to compose sophisticated applications with little training, it can leave applications vulnerable.

Perhaps the most challenging aspect of composable applications is the inability to fully understand the composition, and therefore the security posture, of the application until it is deployed. Only then — when it's too late — are all the contributing elements exposed, including malware and vulnerabilities.

This challenge is causing the embedding of security development expertise into the tools and development platforms, to perform security checks at each stage of development and to combine the component scanning into a composite analysis. Organizations should also be ready to track the provenance of deployed software artifacts to ensure the integrity of mission-critical applications. Because malware can be introduced at virtually any stage of the lifecycle, organizations should be able to establish and track a chain of custody as software moves throughout the lifecycle.

Looking ahead

A longtime contributor of best practices for secure software development, the IBM Rational® Software Delivery Platform — including IBM Rational Team Concert, IBM Rational Asset Manager and the IBM Rational AppScan® family of Web application security solutions — offers features for managing the chain of custody of software artifacts throughout the application lifecycle and can enforce security testing as part of the software development process.

The IBM Tivoli Access Management family of products and WebSphere DataPower SOA Appliances protect applications from unauthorized access and malicious messages.

Correspondingly, at the data level the IBM Optim Data Privacy Solution can integrate with IBM Rational Data Architect to create privacy specifications that can be used across test databases.

The Rational AppScan family of offerings combines application scanning and security checks throughout the phases of the software development lifecycle into a composite analysis of the application security profile on an enterprise scale.

The total average cost to United States companies is $182 per record compromised, equating to an average price tag of $660,000 per company in expenses.

— Ponemon Institute survey, October 2006

Looking ahead

Built on its RealSecure® family of intrusion detection solutions (IDS) products and its Proventia family of IPS offerings, IBM is working to create a new security-consolidating paradigm of network protection. Backed by the IBM ISS X-Force® research and development team, IBM Proventia Network Intrusion Prevention System GX-series offerings can provide protection for physical, virtual and blade-based appliances. Other IBM offerings deliver new classes of protection, such as Web application protection and data loss prevention (DLP), combined with IPS and other functions, in a single appliance.

Working in collaboration with ISS network protection solutions, IBM is creating extensible in-dwelling security within IBM products. In addition, IBM STG and semiconductor teams are working on security acceleration functions in silicon as part of its PRISM project and working to expand the protection ecosystem by creating a framework to integrate third-party protection solutions with unified management.

Trend 7: Protecting the Evolving Network

The need to accommodate bandwidth-intensive applications such as VoIP, streaming video and online gaming has become a race to meet growing demands for speed and bandwidth. With speeds now reaching 10G and beyond and traffic loads hitting unprecedented levels, service providers have increasingly less visibility and knowledge of the traffic going through their networks. As IT policies force more network encryption and virtualization creates new networks inside the server infrastructure, visibility is expected to become even more opaque.

As a consequence, network security should become more elusive, even as new types of attacks emerge. Virtualized environments create the possibility for guest hosts to launch network-based attacks against other hosts. Other attacks likely will target session initiation protocol (SIP) proxy servers, domain name system (DNS) servers and the upper layers of the open system interconnect (OSI) stack, including attacks on application-specific protocols and schema.

Combating these attacks likely will require more than traditional intrusion prevention systems (IPS) and firewall technologies. Addressing these evolving threat requirements should require a total defense-in-depth strategy based on a highly scalable, collaborating security platform with unified and coordinated network, server and end-point protection technologies.

There are 3.3 billion mobile phones in the world today, compared with 1.6 billion Visa cards.

— IBM Global Innovation Outlook[4]

Trend 8: Securing Mobile Devices

Of all the technologies available, the mobile device represents perhaps the greatest intersection between opportunity and risk. Diverse in design and use, and capable of delivering data, applications and services anytime, anywhere, the mobile device has the potential to change the way governments and enterprises conduct high-value, mission-critical transactions.

While the mobile device offers a compelling case as the new prevalent channel for conducting business and primary means for authentication, much work lies in the area of security. Even as they rapidly supplant the PC, mobile phones are increasingly subject to the same types of security attacks – but even less mature at deflecting them.

In the near future, improvements are needed in two key areas: mobile platform security and telecommunications network protection. With mobile platforms becoming more open, the mobile application development environment, deployment processes and run-time environment should be authorized, secure and free of corruption. And as mobile phones are increasingly vulnerable to malware and other types of attacks, telecommunications service providers should augment their network security by monitoring their network traffic for security threats while maintaining optimal service levels.

Looking ahead

Over the years, IBM has pioneered a range of services, offerings and standards to help organizations unlock the potential of the mobile device in a secure and sustainable manner. To help secure the mobile platform, the IBM Lotus® Expeditor family of products offers a turnkey deployment platform that provides a variety of security services such as authentication and encryption for applications running on the platform. The IBM SecureBlue research project is exploring ways to make the hardware components of mobile devices secure and tamperproof.

In the area of telecommunications network security, the IBM BladeCenter® PN41 provides customizable Deep Packet Inspection (DPI)-based security capabilities that telecommunication networks can use to protect mobile devices from malware and other security threats.

Trend 9: Sense-and-Response Physical Security

In the IBM 2008 Global Technology Outlook, we noted the growing demand for low-latency event analysis of physical events for millisecond sense-and-respond reactions. For example, applying RFID stickers to pallets in a supply chain enables IT systems to become aware of the state of the supply chain and raise alerts and take actions as necessary to keep the supply chain running smoothly.

This same sense-and-respond paradigm is now being applied to real-world security. Video analytics enable automated surveillance through object and people recognition, as well as behavioral analysis. In real terms, this allows security officials to program an IT system monitoring a particular camera to detect cars entering a certain area delineated on the screen and staying for longer than 20 minutes without leaving. Or they could perform a metadata-enabled search through an archived video to find a particular type of event such as "a blue sedan crossing this intersection."

Underlying the trend toward this sense-and-respond technology is the idea of giving IT systems a deeper understanding of the semantics of what they're observing. This development likely will correspond to the modeling of more sophisticated behavioral activity models used as baselines for observed activity. As the technology matures, look for video analytics to be widely adopted for both smaller environments and larger, more complex investigations.

As more video cameras are deployed across the globe, however, the limitations are becoming apparent. The most obvious drawback is the human element – that is, a camera can monitor a crowd but someone must monitor the camera. At the same time, human watchers can raise potential privacy issues, particularly where personal information can be compromised. The challenge is to enable IT systems to monitor the cameras in ways that protect the privacy of individuals while recognizing situations that require human attention.

Looking ahead

The IBM Smart Surveillance Solution builds on sense-and-response technology, providing multiple decision-integrating sensors and cameras and extending the querying capabilities of standard digital technology. Designed for a number of industries, it allows organizations to sense and respond to trends and activities based on an open architecture framework that can easily scale to accommodate new monitoring technologies or analytical algorithms.

Summary

This paper has outlined nine trends that will gain increasing prominence in the next two to five years. Given these trends, it is likely that these next few years have the potential to bring tremendous risk. But they can also usher in a wealth of opportunities. It's how the risk is managed that should determine how an organization thrives – or fails – in the face of emerging technologies.

While most security vendors focus on and manage one area of risk, IBM's approach is to strategically manage risk end-to-end across all areas of the organization. This strategy allows organizations to better understand and prioritize risks and vulnerabilities based on their potential to disrupt critical business processes.

Through world-class solutions that address risk across each aspect of your business, IBM can help you build a strong security posture across the organization and position you to reap the rewards of emerging technology trends.

For more information

To learn more about emerging security technology trends, contact your IBM representative or IBM Business Partner, or visit **ibm.com**

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
October 2008
All Rights Reserved

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

[1] "The Data Center 'Implosion Explosion' … and the Need to Move to a New Enterprise Data Center Model," www-03.ibm.com/systems/resources/systems_optimizeit_datacenter_pdf_nedc.pdf

[2] IDC Worldwide Identity and Access Management 2008-2012 Forecast and 2007 Vendor Shares, August 2008 (Doc #213650).

[3] http://www.privacyrights.org/

[4] ibm.com/gio