Leveraging innovative security solutions for banking and financial markets

Establishing a security-rich environment amidst business competition and pervasive Internet threats
Managing threats, reducing fraud and maintaining client trust

Complex industry regulations and threats to revenue, reputation and operations have converged to make security and fraud chief concerns for financial companies. At the same time, many financial institutions are integrating with partners and enabling interactive customer services to support aggressive growth in today’s competitive business climate.

New business and technology initiatives carry inherent IT risk and must be balanced with the ongoing need to preserve trust and protect reputation. Only a robust IT security program enables banks and financial markets organizations to extend services securely. To be successful, security management should be part of a broader model of managing operational risk and fraud without adversely impacting business processes or customer services.

As one of the earliest adopters of IT security technology, the financial sector far outpaces many other industries in network and information protection. Even so, the growing complexity of the IT environment and the subsequent increase in security point products have made it difficult to integrate a holistic security strategy with overall business planning. All the while, security threats are evolving, vulnerabilities are increasing rapidly, and data leakage continues to present significant risk in terms of liability, cost and impact on reputation.

You may already be replacing obsolete security solutions and/or layering on additional security in what seems like a never-ending cycle. But even when you operate with well-defined business strategies, your security may consist primarily of endpoint solutions that lack integration. With finite security dollars, you may wonder where to invest next, how to prioritize security requirements according to best practices and how to leverage past security investments.

More than ever, you may recognize the need to optimize security investments by taking a more holistic view of threat mitigation and developing effective policies using commonly available tool sets. Financial executives, chief information security officers and IT staff understand the high stakes of security, but they often lack the real-time metrics and operational reporting to support security at the same level as other IT initiatives. Despite such challenges, successful and protected financial institutions continue to focus on secure IT efforts that help differentiate the business, accelerate threat management, and meet government, industry and business partner compliance requirements.
Using the right approach to IT security in banking and financial organizations
With a long history of serving banks and financial markets organizations, IBM recognizes the following best-practice IT security strategies and tactics as the building blocks needed to achieve a strong security foundation that can easily integrate with your business goals and strategies.

Assess your security and compliance posture
To transform existing IT security investments into an integrated, effective model that meets regulatory requirements and internal controls, you must first understand your current environment. Establishing a baseline for security remains a critical first step in building a strong IT security foundation.

To gain a greater understanding of your security and compliance posture, IBM recommends these steps:

- Perform vulnerability assessments and penetration testing, allowing you to conduct a detailed analysis of existing weaknesses and potential inlets for malicious activity.
- Leverage security assessments of your applications, governance and IT controls to determine your level of protection against potential threats. Assessments make you aware of problems ahead of auditors, and help establish a roadmap to address any discovered security vulnerabilities.

Improve and harden your enterprise security
Once you’ve established a baseline for security and identified weaknesses for remediation, a logical next step is to improve and harden your network and application design by:

- Designing security-rich access zones and applying whitelisting, blacklisting and other advanced techniques to protect your information assets from theft and misuse
- Using advanced security technologies such as intrusion prevention and anomaly detection to help mitigate threats.

Enhance your identity and access management
With insider threats on the rise and compliance requirements a major concern, identity and access management form critical components of a holistic security strategy. The IBM recommended approach involves:

- Managing user rights and identities throughout their entire lifecycle
- Using strong authentication to help verify that only authorized individuals can access certain resources
- Evaluating user activity to help ensure optimal threat management and demonstrate due diligence with compliance standards.

Many banks and financial organizations are caught in a balancing act between business and security priorities

Business priorities
1. Maintaining competitive advantage through customer and marketplace differentiation
2. Attracting and retaining new customers
3. Building a responsive and flexible organization

Security priorities*
1. Defining a unified security strategy
2. Developing defenses against complex external threats
3. Protecting data throughout its lifecycle

By enhancing your identity and access management, you can help reduce the risk of information theft while enabling connectivity for employees and trusted third parties and enhancing customer interaction. In addition, you can more proactively identify and address inappropriate behavior and document the effectiveness of security policies and identity-related controls.

**Increase data security**

Ultimately, you want to protect information assets and increase data security at the same time. To do this, you must first establish a core data security architecture by:

- Setting information asset profiles to determine where critical data resides, who can access it and how well it’s protected
- Applying and managing a comprehensive encryption strategy to help keep private information confidential and meet compliance mandates
- Implementing enterprise key management for encryption and data protection across the enterprise—from storage on local, removable devices, through servers and hosts, to long-term backup and storage on tape
- Managing the disposal of data-bearing media, whether it’s paper, magnetic media or optical media, to help protect your and your client’s confidentiality for the long term.

**Address physical security requirements**

Physical security threats are a harsh reality. To help offset the risks, you can create an enterprisewide, universal ID solution by:

- Integrating identity management systems with physical security systems
- Deploying a digital video surveillance strategy and architecture to help reduce physical threats and mitigate the inefficiencies of analog video technology
- Engaging in contingency planning to help enhance your ability to deal with critical infrastructure and homeland security crises.

**Monitor risk and compliance**

Continuous monitoring of your risk and compliance is essential to driving effective IT security and brings financial institutions full circle to the first step of establishing a security baseline. Continuous monitoring enables you to:

- Work from a risk and privacy strategy to make improvements, and then measure those improvements and report the results
- Use automated tools to create reports that not only demonstrate effective threat mitigation, but also help simplify various components of compliance testing and reporting.

---

**SECURITY SOLUTIONS FROM IBM**

<table>
<thead>
<tr>
<th>Governance</th>
<th>Data security</th>
<th>Threat mitigation</th>
<th>Physical security</th>
<th>Identity and access management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides risk management, security governance and regulatory compliance</td>
<td>Enables widespread electronic collaboration while protecting data at rest, in motion, in use and at the endpoint</td>
<td>Provides on demand protection to stay ahead of emerging threats</td>
<td>Provides an integrated video surveillance and security solution that can include industry-standard components</td>
<td>Provides planning and implementation for identity and access management needs</td>
</tr>
</tbody>
</table>

IBM takes a holistic approach to security and privacy with solutions that can help organizations like yours to lower costs, accelerate protection and reduce overall threats.
Address your security needs—from the network core to the perimeter—with innovative solutions from IBM

IBM’s security solutions help financial institutions remain ahead of the onslaught of IT threats. These solutions can help you lower costs, accelerate protection and reduce overall threats. Following a well-established framework for securing financial institutions, IBM works directly with clients to prioritize IT security projects and build a roadmap for implementation.

IBM offers a comprehensive approach to securing the IT environment. Depending on your unique needs, our security solutions can help you:

- Assess your security posture from a people, process, technology, risk and compliance perspective
- Protect valuable technology and information assets—preemptively
- Defend your IT environment against threats
- Monitor your IT landscape for security changes
- Control risk within your organization as it relates to technology and overall compliance.

Security solutions from IBM include hardware, software, consulting and managed services delivered through a full range of offerings that cover the following areas:

Security governance solutions
Security governance solutions from IBM go beyond the technical perspective to evaluate existing security practices in light of current business requirements and future objectives. This helps you address security in a holistic and cost-effective manner while potentially accelerating your return on investment. The knowledge gained from IBM’s security governance solutions can help you allocate funds and resources to manage information security threats more effectively. With our regulatory and standards compliance services, you can assess and develop operational business models and processes that help you establish, manage, monitor and maintain effective enterprise IT security.

Security governance solutions from IBM encompass security risk management, program design and management, regulatory compliance services, privacy services, and security education and training services designed to drive an effective, integrated security program that meets your business and IT needs.

Threat mitigation solutions
Threat mitigation solutions from IBM can help you maximize existing security investments while reducing cost and complexity. Encompassing the IBM Internet Security Systems™ suite of products and services, threat mitigation offerings include network protection, endpoint protection, enhanced application integrity, as well as security and vulnerability management. Fueled by in-depth security intelligence gathered by the IBM Internet Security Systems X-Force® research and development team—a world-renowned authority on global Internet threats and vulnerabilities—IBM Internet Security Systems solutions can offer proven protection for your valuable assets.

Our threat mitigation solutions can help you better understand your current security posture and develop strategies that can optimize future security investments. Plus, threat mitigation solutions from IBM are designed to anticipate and guard against attacks on the network every hour of every day throughout the year—before they can adversely affect your business. More importantly, advanced threat prevention technologies from IBM are designed to automatically protect your network from data loss and attack without requiring significant management or expertise from your internal IT staff.

Identity and access management solutions
Identity management solutions from IBM help organizations like yours achieve a more rapid return on investment by bringing users, systems and applications online quickly. In addition, you will be able to effectively and securely manage users, and access rights and privacy preferences throughout the identity lifecycle. IBM can help you design, implement, deploy and maintain a seamless and integrated
identity management system that’s designed to reduce the costs of supporting multiple systems and identities across the organization. Our identity management solutions protect valuable data and resources while enhancing the user experience through single sign-on and automated password reset capabilities. In addition, IBM solutions facilitate the sharing of identities between partners, which can enhance growth initiatives. Offerings in this space leverage industry-leading IBM Tivoli® software to help you define and maintain access policies and user rights, and monitor and report actual user activity to facilitate compliance initiatives.

Identity and access management solutions from IBM provide assessment, strategy, proofing, information lifecycle management (ILM) and authentication to facilitate regulatory compliance while providing security-rich access to the right people.

Data security solutions
Whether your data is in transit between endpoints or resting at an endpoint, data security solutions from IBM can enable widespread electronic collaboration while helping to protect your data from existing and emerging threats. The holistic approach from IBM establishes a core data security architecture that integrates with leading components from IBM and other vendors to help protect key data assets and business transactions. Built on world-leading research and development, our data security solutions can enable you to take a more proactive security posture, rather than reacting to security events.

IBM’s integrated data security solutions include high-performance, transparent encryption offerings to help protect data from unauthorized physical access and inadvertent data exposure when media is lost or stolen or when systems are decommissioned from service. The following are also part of the data security solution portfolio provided by IBM:

- Activity compliance monitoring and enforcement
- Enterprise content protection
- Enterprise key management tools for encryption solutions
- Mobile endpoint protection

Physical security solutions
IBM integrates digital video surveillance technology from marketplace leaders with advanced video analytics developed by IBM to create a powerful physical security solution. Until recently, financial organizations were limited to analog surveillance solutions—which can be labor intensive, difficult to maintain and expand, and limited in their capability to provide alerts and post-event analysis. With the digital video surveillance solution from IBM, you can gain a more cost-effective, scalable and integrated way to capture, store, retrieve and manage digital video content. Plus, you can take advantage of automated, intelligent analysis to help improve real-time or post-event decisions and actions. Your organization can benefit from the ability to:

- Respond more effectively to threats in the physical environment
- Enhance the security of main and branch sites
- Increase operational efficiency
- Find new ways to extract useful business information from video surveillance data
- Boost client satisfaction by alerting management to long customer lines
- Provide analyses of customer responses to marketing displays
- Generate alerts regarding automated teller machine (ATM) tampering
- Identify employees or high-wealth customers using facial recognition technology.

IBM—your trusted security adviser
As an industry-leading IT integrator and partner to global organizations, IBM is an established technology adviser to banks and financial institutions and is able to bring superior security tools to the financial industry.

IBM takes threats seriously—and it has the research to prove it. The IBM Internet Security Systems X-Force team is a world-renowned authority in threat and vulnerability discovery
and analysis, and regularly conducts primary security research. IBM monitors the Internet threat landscape and actively participates in setting the daily Internet threat level with the United States Department of Homeland Security. Plus, IBM security experts conduct global threat monitoring every day, year-round, from five security operations centers (SOCs) located around the globe, and manage tens of thousands of security sensors for clients worldwide.

When you are looking for a trusted technology adviser that can assume security management on an outsourced or out-tasked basis, IBM is ideally suited to help you establish and maintain a security program, regardless of the model you choose to deploy. IBM also provides direct access to expert security consultants who understand attack design, underlying vulnerabilities, security policies and compliance mandates. Addressing your needs from physical and data security to identity management and compliance audits, IBM provides skilled consultants to complement the efforts of your internal staff or to provide comprehensive managed security services.

IBM provides offerings that are designed to enhance your organization’s security posture to whatever level is required. Rather than delivering only hardware or software, the IBM security portfolio spans people, process and technology — just as any effective IT initiative would. No matter where your organization falls along the security continuum, IBM solutions can help you reduce risk and alleviate the pains associated with security.

**For more information**
To learn more about how security solutions from IBM can help protect your organization more effectively and efficiently — and to find the IBM security entry point that is right for your organization — contact your IBM representative or IBM Business Partner, or visit:

[ibm.com/security](http://ibm.com/security)