Information technology risk management for financial institutions

Prepared by:

Hussain Hasan, Principal, RSM US LLP
hussian.hasan@rsmus.com, +1 847 413 6287

Doug Underwood, Principal, RSM US LLP
doug.underwood@rsmus.com, +1 612 376 9210

Loras Even, Principal, RSM US LLP
loras.evan@rsmus.com, +1 319 274 8541

Sudhir Kondisetty, Principal,RSM US LLP
sudhir.kondisetty@rsmus.com, +1 215 648 3121

Information technology risks and threats

In today's ever-changing financial institution technological landscape, evaluating risk and controls is of tantamount importance. With an increased number of internal and external threats to your institution, it is more important than ever to protect yourself against a breach of your IT systems.

Your sensitive customer information could be at risk due to an increasing wave of IT attacks. Information has become a very valuable commodity to organized criminals and the reputation of your institution can suffer tremendously if your information is compromised. Technological advancements like social media/networking, cloud computing and virtualization along with threats such as data leakage, pose a new wave of risks and threats to financial institutions.

The theft of information is becoming more widespread and less complicated to carry out. Symantec created 2,895,802 new malicious code signatures in 2009, a 71 percent increase over 2008; the 2009 figure represents 51 percent of all malicious code signatures ever created by Symantec.

According to the 2009 CSI/FBI Computer Crime & Security Survey, 27 percent of organizations had identified themselves as the recipient of a targeted attack. Verizon investigated more than 500 breach investigations and concluded that more than half required little to no skill to perpetrate.

And in 2009, the survey also indicated:

- Respondents reported big jumps in incidence of password sniffing, financial fraud and malware infection.
- One-third of respondents' organizations were fraudulently represented as the sender of a phishing message.
- Twenty-five percent of respondents felt that over 60 percent of their financial losses were due to non-malicious actions by insiders.
- Most respondents felt their investment in end-user security awareness training was inadequate, but most felt their investments in other components of their security program were adequate.
- When asked what actions were taken following a security incident, 22 percent of respondents stated that they notified individuals whose personal information was breached, and 17 percent stated that they provided new security services to users or customers.
- When asked what security solutions ranked highest on their wish lists, many respondents named tools that would improve their visibility — better log management, security information and event management, security data visualization, security dashboards and the like.
- Respondents generally said that regulatory compliance efforts have had a positive effect on their organization's security programs.

Social security numbers, financial institution and credit card information, email accounts and addresses are all information that hackers search out, and chances are, much of this customer information can be found on your servers. All of this information can be used fraudulently, or sold to another party that will make criminal use of it, such as identity theft.

Types of attacks

Attacks can come from a variety of sources, with Web attacks occurring slightly more often than those that come directly to your network. Tactics such as spam, phishing emails and viruses sent as attachments are very prevalent, as well as infected websites that attempt to launch a virus onto a user's computer or infiltrate the network as a whole.

Industry studies have shown that roughly 200,000 more records per month were compromised in 2007 than in 2006. Spam emails that may include phishing content or viruses account for an average of 1.2 billion messages per week (71 percent of all email) and are most commonly associated with financial goods and services.

If an attacker discovers a vulnerability in your IT security, they will continue to exploit it, possibly with escalating degrees of damage. If one facet of your security has been neglected, there are likely other holes that may exist.

The use of Botnets has also been on the rise in recent years, as a central location will control other computers remotely, running a network to distribute and execute malicious software. There has been a recent international effort to thwart Botnets, but they still remain a significant threat.

Internal threats

Many businesses concentrate on outside threats, but may forget about ones that are in their own offices. With the current difficult economy, fraudulent behavior by employees and insider threat is sharply on the rise.

Common issues

There are several issues that can be easily corrected that can lead to security breaches. Those include:

- Inadequate training — Make sure that your employees know what to look for in a potential attack
- Poorly chosen or infrequently changed passwords — Passwords must be of a certain length, include certain characters and be changed periodically
- Remove or disable terminated employee user accounts ASAP — A former employee who might hold a grudge against your organization should not have an opportunity to access your systems
- Lack of management attention to security issues — Reinforce the importance of information security and follow up on any planned initiatives
- Instill a sense of urgency — If there is any suspicion of an issue, it must be investigated

Furthermore, the volume of FDIC Financial Institution Letters (FIL) issued recently highlight the changing IT landscape and risks or threats that can have a dramatic impact on a financial institution. Some of those topics include:

- Identity theft
- Remote deposit capture
- Third party/vendor/payment processor relationships
- Influenza/pandemic planning
- Internet banking/e-Commerce
- Voice over Internet Protocol (VOIP)
- Spyware
- Phishing/Pharming
- Proper disposal of customer information
- Virtualization

The increased monetary value of information has escalated the profile of a potential attacker from a "script kiddie" to a professional attacker. Your information security capabilities should follow suit and match the threat level that is apparent today, while also planning for future attacks. The vast majority of data is compromised by poor implementation of proper controls, not through hacker implementation. So what can your organization do to protect itself?

What can be done?

Financial institutions should consider the development or enhancement of a comprehensive information technology risk management program, designed to ensure the security and confidentiality of customer information, anticipate future threats and protect against unauthorized access that could result in substantial harm or inconvenience. Involve the board to develop a written program that assigns responsibility for completing tasks and sets deadlines.

It is important to assess your specific risks, envisioning reasonably foreseeable internal and external threats. Work with your IT experts or an outside consultant to design a program that considers preventative, detective and corrective controls.

Supplementing your current IT security systems may sound like it is an expensive task, especially in a tenuous economy and with funding difficult to predict from month to month. However, it may be less of an expense than originally thought. Many IT systems are not being used to their full potential, and have security capabilities that are not being taken advantage of. The software can be adjusted to increase the sensitivity to a higher level or look for specific viruses or malware. Many very inexpensive and effective security software options are also available.

There is big money involved with stolen personal information. As that continues, it is imperative that your organization takes protective measures to guard your IT systems. Cost is always going to be a primary concern, but it is difficult to put a price tag on the value of your reputation and the sensitive information of the institution.

Understanding threats and risks to an institution's IT environment will help to build and implement a solid risk management program, which begins with an evaluation of risks and threats – a risk assessment.

Managing IT risk through a risk management program

Successful and effective risk management is the basis of successful and effective IT security. Due to the reality of limited resources and nearly unlimited threats, a reasonable decision must be made concerning the allocation of resources to protect systems. Risk management practices allow the organization to protect information and business processes commensurate with their value. To ensure the maximum value of risk management, it must be consistent and repeatable, while focusing on measurable reductions in risk. Establishing and utilizing an effective, high quality risk management process and basing the information security activities of the institution on this process will lead to an effective information security program across the institution.

The basis of an IT risk management program is an assessment of the risks that may have a substantial impact on the institution as a whole, whether they are financial, strategic, legal/regulatory, reputational or a combination. An effective IT risk assessment and risk-based decisions require IT risk to be expressed in unambiguous and clear, business-relevant terms. Effective risk management requires a mutual understanding between IT and the business over which risk needs to be managed and why. All key stakeholders must have the ability to understand and express how adverse events may affect business objectives. This means that:

- An IT person should understand how IT-related failures or events can impact objectives and cause direct or indirect loss to the institution.
- A business process owner should understand how IT-related failures or events can affect key services and processes.

The link between IT risk scenarios and ultimate business impact should be established to understand the effects of adverse events. Several techniques and options exist that can help the enterprise to describe IT risk in business terms.

Standards and frameworks

Because so many security and control standards exist, it is often difficult to determine which best applies to a financial institution. Generic standards offer the most comprehensive view, but these often require security measures that are inappropriate in one industry or another. They fail to take into account your specific context. The best approach may be to evaluate a number of frameworks and determine which best suits your institution.

Various risk standards and frameworks include:

Framework	Standard
COSO ERM	AS/NZS 4360
Val IT (from ISACA)	ISO 31000
Risk IT (from ISACA)	ISO 2700x
Basel II	ISF (The Standard of Good Practice for Information Security)
OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)	NIST 800-30

Understanding the assessment of IT risks

The threat and risk assessment process is not a means to an end. It is a continual process that once started should be reviewed regularly to ensure that the protection mechanisms currently in place still meet the required objectives. The assessment should adequately address the security requirements of the organization in terms of confidentiality, integrity and availability (CIA). The threat and risk assessment should be an integral part of the overall life cycle of the infrastructure.

Institutions that do not perform a threat and risk assessment are leaving themselves open to situations that could disrupt, damage or destroy their ability to conduct business. Therefore, the importance of performing such an assessment must be realized by both the staff supporting the infrastructure and those that rely upon it for their day-to-day business.

The scope of a risk assessment should include:

- An institution-wide analysis of internal and external threats and vulnerabilities to confidential customer information
- The likelihood and impact of identified threats and vulnerabilities
- The sufficiency of policies, procedures and customer information systems to control risks

Besides being a sound business practice, most financial institutions are mandated to perform a risk assessment of information technology infrastructure by, among other guidance, FDIC FIL-81-2005. The FIL states:

> *On June 30, 2005, the Federal Deposit Insurance Corporation (FDIC) implemented a new Information Technology Risk Management Program (IT-RMP) for conducting IT examinations of FDIC-supervised financial institutions. IT-RMP examination procedures apply to all FDIC-supervised banks, regardless of size, technical complexity or prior examination rating. The former IT-MERIT (Maximum Efficiency, Risk-Focused, Institution Targeted) procedures and related work programs have been rescinded. IT-RMP procedures focus on the financial institution's information security program and risk-management practices for securing information assets. These risk-management practices include:*
>
> - *Risk assessment*
> - *Operations security and risk management*
> - *Audit and independent review*
> - *Disaster recovery and business continuity*
> - *Compliance with Part 364, Appendix B of the FDIC's Rules and Regulations*

Unfortunately, what the FIL does not do is define a specific standard for performing the risk assessment.

There are many risk assessment methodologies available from which to choose; for example, Institute of Internal Auditor (IIA) GAIT — Guide to the Assessment of Information Technology Risk (Methodology) or CRAMM — CCTA Risk Analysis and Methodology Method (Methodology). Methodologies range from simple classifications of high, medium and low, based on the management's judgment, to complex and apparently scientific calculations to provide a numeric risk rating. Practitioners should consider the level of complexity and detail appropriate for the institution.

All risk assessment methodologies rely on subjective judgments at some point in the process (e.g. for assigning weightings to the various parameters). The practitioner should identify the subjective decisions required to use a particular methodology and consider whether these judgments can be made and validated to an appropriate level of accuracy.

Basically, you want to identify all operational systems, as well as their inputs and outputs. Next, take a look at your exposure to loss, unauthorized access, excessive downtime, etc. Then, begin to assess the risk to your financial institution's operations if one or more of your considered risk scenarios plays out.

Measuring IT risk calls for different approaches based on the situation. You can take a qualitative or quantitative approach. For example, if you are referring to performing the risk assessment for GLBA, you could take a qualitative approach and write a narrative of the assessment, assigning risk categories (e.g., high, medium, low) to each area. Alternatively, you could take a quantitative approach, assigning values based on: 1) The Threat Likelihood/ Probability of Occurrence, and; 2) The Magnitude of Impact. These values can be multiplied to obtain a risk ranking.

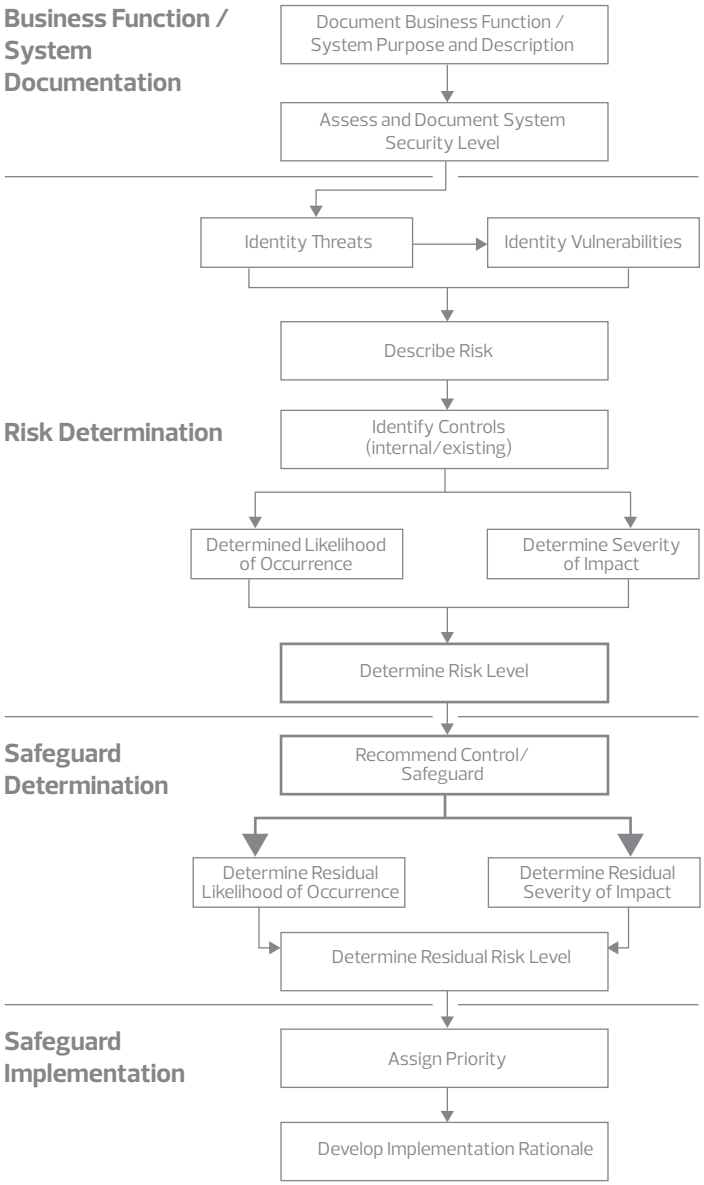
Each individual area can then be categorized into a risk summary. Subsequently, you can identify which risk areas you plan to mitigate through your Risk Mitigation Action Plan. This also serves as an excellent tool for board reporting and monitoring the plan's progress.

Another approach to IT risk assessment involves considering the financial institution's complete IT environment and related sections to be included in the risk assessment. This approach allows a more comprehensive, yet general view of IT risk.

Performing an IT risk assessment

All risk assessments are processes. Typically, the better your processes are (they should be clearly defined and repeatable) the better, or more accurate your results will be. The FFIEC Mandate of October 2005 required that the electronic banking risk assessment be completed by December of 2006, but it would be naive to assume that it will not be required on an ongoing basis.

You can see the basic principles of a risk assessment depicted in the following figure. The process contains the critical elements of a risk assessment process and provides a reasonable baseline:



Risk determination

The risk determination process assumes that specific threats and vulnerabilities have already been identified. In order to identify threats and vulnerabilities, the institution must:

- Identify potential threats to the business function, information, information systems and supporting business processes and resources that could affect the availability and functionality of the system.
- Identify the system weaknesses that could be exploited associated with the threat/vulnerability pair.

Some common threat/vulnerability pairs could include:

Threat	Vulnerability
Arson	· Bombs · Malicious intent
Corruption by system, system errors or failures	· System failures · System errors
Data/system contamination	· Inappropriate data access · Cross-site scripting attacks
Eavesdropping	· Unauthorized disclosure
Environmental conditions	· Poor ventilation and air conditioning · Water leaks · Humidity levels · Overheating · Extreme cold · Sewer backup
Espionage	· Bugs/wire taps · Bribing/blackmailing employees · On-site contractors and other legitimate business associates
Hardware/equipment failure	· Unanticipated device failure
Hazardous material accident	· Train derailment · Interstate accident · Office cleaning chemicals · Spilling materials on equipment
Impersonation	· Misuse of physical access methods · Use of others' identification and authentication information

Threat	Vulnerability
Improper disposal of sensitive media/scavenging	· Residual data left on PC's · Improper disposal of hard copy data · Improper disposal of media storage devices such as tapes · Improper disposal of voided checks · Improper disposal of voided MSN's/ remittance statements
Inadvertent acts or carelessness	· Failure to inactivate passwords/user accounts/etc. when an employee is terminated · Failure to obtain access cards from terminated employees/failure to remove access from badge system · Piggy-backing · Incorrect physical access · Buffer overflow · Periods when data is unprotected
Insertion of malicious code, software or database modification	· Unauthorized addition or modification of a system's configuration
Installation errors	· Poor installation procedures for hardware or software
Intrusion or unauthorized access to system resources	· Unauthorized access to system resources for malicious or non-malicious (curiosity seeker) reasons
Misuse of known software weaknesses	· Bypassing security
Natural disaster	· Earthquake · Flood · Tornado/high winds
Omissions	· Failure to perform essential security functions
Physical cable damage	· Lightning strikes · Animals · Disgruntled employees · Random crimes
Power fluctuation	· Power spike · Power surge · Brownout · Blackout
Procedural violation	· Refusal to carry out work-related tasks
Riot/civil disorder	· Blocking access · Refusal to carry out work-related tasks
Saturation of communications or resources	· System components being intentionally flooded to their maximum capacity
Secondary disasters	· Broken water pipes · Spilled chemicals
Segregation of duties	· Information systems job descriptions do not reflect segregation of duties
Shoulder surfing	· Employees · Visitors · Remote dial-up access
Tampering	· Unauthorized modifications of equipment or systems
Telecommuting	· Lack of companywide telecommuting standards (policy) · Inadequate perimeter access controls
Terrorism	· Terrorist acts
Theft, sabotage, vandalism or physical intrusions	· System sabotage · Destruction of hardware or facility · Computer abuse · Piggy-backing · Vendor access
User abuse	· Excessive personal system use · Unauthorized searches
Vendor license noncompliance	· Owning the improper number and/or type of licenses for software products

Level of impact

Once threats and vulnerabilities have been identified, an analysis of the potential impact of each threat to the business function is performed to determine risk. Common steps usually include:

- Analyzing the potential business impact of each risk for the financial institution
- Identifying existing controls to reduce the risk of threat occurrence or for a threat exploiting a related vulnerability
- Determining the likelihood of a threat occurrence or a threat exploiting a related vulnerability given the existing controls

- Determining the severity of impact on the business/system function by threat occurrence or by an exploited vulnerability
- Determining the Risk Level given the existing controls

The goal of risk determination is to calculate the level of risk for each threat/vulnerability pair based on:

- The likelihood of a threat exploiting a vulnerability
- The severity of impact that the exploited vulnerability would have on the system, its data and its business function in terms of loss of CIA

The risk can be expressed in terms of the likelihood of threat occurrence/threat exploiting vulnerability and the severity of impact. Mathematically, the Risk Level is equal to the Likelihood of Occurrence multiplied by Impact Severity as follows:

Risk Level = Likelihood of Occurrence x Impact Severity

The risk may be increased to a higher level depending on the system security level and the level of compromise if a threat is realized. However, the risk level cannot be lowered, unless the likelihood of occurrence and severity of impact are also changed.

Control identification

The next step of a risk assessment process requires the identification of additional controls, safeguards or corrective actions to minimize the threat exposure and vulnerability exploitation for each threat/vulnerability pair identified, resulting in moderate or high risk levels.

Controls/safeguards for threat/vulnerability pairs with low risk level normally would not need to be identified, as the goal of a risk assessment is to reduce a risk level to low. The recommended goal of the control would be to reduce the risk level for business and system risks. The residual risk level is determined assuming full implementation of the recommended controls. When identifying controls, focus on the following:

- **Control descriptions** – Identify the controls/safeguards to reduce the risk level of an identified threat/vulnerability pair, if the risk level is moderate or high
- **Residual likelihood of occurrence** – Determine the residual likelihood of occurrence of the threat if the recommended safeguard is implemented
- **Residual impact severity** – Determine the residual impact severity of the exploited vulnerability once the recommended safeguard is implemented
- **Residual risk level** – Determine the residual risk level for the system

Control implementation and ongoing review

The final stage of the process is the implementation and ongoing review of controls that protect the institution against identified risks. This is where an audit or review of controls validates the implementation and effectiveness of the stated controls. The audit or review of controls along with regular maintenance of the risk assessment occurs typically on an annual basis (or after the implementation of a major control/application change) to complete an overall risk management program.

What's best for my environment?

In deciding which is the most appropriate risk assessment methodology, institutions and their internal auditors should consider factors such as:

- The type of information required to be collected (some systems use financial effects as the only measure – this is not always appropriate for information technology reviews)
- The cost of software or other licenses required to use the methodology
- The extent to which the information required is already available
- The amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise)
- The opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits
- The willingness of management to accept the methodology as the means of determining the type and level of audit work carried out

Summary

The importance of a continual IT risk management process, including risk assessment, is further emphasized by emerging IT trends like social media/networking, cloud computing and virtualization along with threats such as data leakage, stressing the need for ongoing evaluation of the new wave of risks and threats to financial institutions.

Emerging it trends and risks

The adoption of emerging technologies by the financial industry has grown exponentially in recent years. New technologies that enable new functions and interconnect the business world have exploded in the general public and are now being thrust into the business world often without thoroughly examining the risks they pose. In today's economy, the opportunity for efficiency and growth is expedited by customer demand. Security risks arise when institutions rush to implement new technologies to meet the ever-changing needs of the marketplace without first reviewing the impact to their existing risk management plans. Technology also changes so quickly that it can evolve before the risks are fully known.

The following pages explore the risks of emerging technologies like cloud computing, web applications and social networking, and provide practical guidance for mitigating those risks. They also address certain IT trends being seen in the marketplace like data leakage and web application security, topics that frequently cause difficulty in maintaining a secure technology landscape, particularly at financial institutions.

Implementing social media sites

The power of social media and its influence on growth in the financial industry is mesmerizing. However, equally compelling is the conspicuous absence of guidance from regulators who may be holding back many financial institutions from taking the plunge.

Social media sites such as Facebook and Twitter are energetic, dynamic and interactive. When compared to traditional sites where members must seek out the content and then mull over pages of information, social media sites serve up and dish out content to the members in compact, snack-sized portions. Social media sites are updated daily, or even hourly, with new postings to interact directly with members.

Twitter so recognizes the needs of businesses wanting to reach customers using social media channels that it set up an extensive website to facilitate the process of implementing a successful presence. The business-focused website discusses best practices and includes several case studies to evaluate.

Security risks

There are fundamental security risks common to social media sites. Understanding the risks and applying controls to address the impact of these risks is imperative to establishing a successful social media presence. Social media site security is facilitated by the service provider, which means that the security controls, or lack thereof, are limited to the predefined options. These options should be used to their fullest extent.

Foremost on the list is to use strong password controls. Ensure the password is unique to the social media site and is long and complex, changing the password regularly. Because the website is hosted on the provider's servers, everyone subscribing to the service is subject to outages and hacker attacks waged against the provider's server infrastructure such as denial of service and malware attacks.

Regulatory guidance

Not until January of this year has any guidance been published by a regulatory organization of the financial industry. The Financial Industry Regulatory Authority (FINRA), an independent regulator for securities firms, published Regulatory Notice 10-06, Guidance on Blogs and Social Networking Web Sites. The guidance is designed to protect investors against false or misleading claims on social media sites. It is also intended to help organizations develop their own policies and procedures that are in compliance with the regulatory requirements specified by the notice.

Regulatory Notice 10-06 centers on the following responsibilities:

1. Record-keeping and retention of business-related communications
2. Recommendations posted to buy or sell securities that are suitable and appropriate to the investors reading the posts
3. Supervisory review of communications posted that are compliant
4. Management of third-party postings on the firm's social media sites

The FINRA regulatory notice is targeted at Securities and Exchange Commission-regulated firms, and it communicates a guidance framework that financial institutions may adapt to their own supervisory and compliance programs.

Record-keeping – The guidance extends existing requirements to retain all business-related communications with the public to include social media websites. For publicly available social media sites, correspondence may be categorized as advertising or sales literature and be subject to pre-approval, filing and a 3-year retention from the date of the latest posting.

Suitability – The suitability rule is related to recommendations posted about buying or selling securities. The rule stipulates that any recommendation made be suitable for the customer or investor who sees it. Complying with the suitability rule becomes challenging when you consider the potential audience of followers on the social media site who may view the posted communication.

Supervisory review – This rule appears to be rooted in FINRA rule 3010, which includes having written procedures for the control of the process, and the principal review and approval of electronic correspondence. This may seem diametrically opposed to the customer expectation of immediacy on social media websites. However, certain provisions may be implemented into policies and procedures to not require prior principal approval related to "unscripted remarks" in certain situations when engaging in interactive communication with the customer. For example, interactive Facebook wall posts, direct messages and Twitter tweets with customers are usually considered unscripted correspondence. Depending on the subject matter and the financial institution's risk appetite, almost all other canned or static posts will require pre-approval. To keep the site responsive, having a good database or cache of pre-approved posts may be a good solution to ensure the site is active.

Third-party postings – Unless a financial institution is working with a third-party to collaborate on or endorse the content of a post for the Facebook wall or Twitter page, third-party posts are generally not considered a public correspondence by the financial institution. Any collaborative efforts with third-party entities will obligate compliance with all applicable social media rules in the guidance by the financial institution.

Social media sites pose significant compliance risks, due in part to the heightened focus on consumer protection regulations. The departmental organization charged with developing and managing the social media site content must either be highly proficient with compliance requirements or else work closely with the compliance department before adding any information to such sites. The compliance requirements applicable to the social media sites include advertising and records retention requirements.

For credit unions, the primary advertising regulations affecting social media sites are Regulation Z and NCUA Rules and Regulations Part 707 (Truth in Savings). Violations of both requirements on social media sites are common. If your social media site contains a trigger term for loan products or share accounts, you are required to include further disclosures. For Regulation Z, one of the most common trigger terms we see on social networking sites is the APR for home equity lines of credit (HELOC). For instance, consider this Facebook posting: "HELOCs at 3.00% APR!" "3.00% APR" is a trigger term requiring several significant disclosures, including whether the rate is variable, if there are any membership or participation fees, and if any fees are considered a finance charge.

Similar to the FINRA requirements, NCUA Rules and Regulations Part 707 and Regulation Z requires retention for two years evidence of compliance.

Have a strategy

The first step in starting a social media site is to have a plan. As obvious as that sounds, it is an all too often overlooked prerequisite to an effective implementation. As with any other business venture, starting with a strategy can help ensure that the following are in place:

- Measurable value derived from implementing social media
- Executive management participation
- A mission statement and goals
- Recognition of what the site will promote or advertise
- Awareness of the services that will be offered
- An understanding of the business, member, security and compliance risks
- Assigned responsibilities
- Monitoring and the review of controls

Oversight

As more regulatory guidance becomes available and the complexity of social media evolves over time, incorporating social media with information technology governance provides a scalable solution to manage policies, standards and procedures. Controls should be monitored and audited for deficiencies. The scope of review should include, but not be limited to the following objectives:

- Compliance with information technology controls
- Compliance with regulatory standards
- Approval processes for postings
- Evaluation of monitoring controls
- Page reviews to ensure that content was not compromised
- Fan or friend profiles that appear appropriate
- External link destinations that were not compromised, broken or include malware for attacks

Having a strategy in place before implementing a social media presence on the Internet can improve success dramatically. A social media strategy will align the goals of the site with expectations of the financial institution and it will provide needed controls over operations, security and compliance.

Data leakage primer: Securing the enterprise

In the world of information security, data leakage is the new black, occurring at an increased rate in recent years. Security management faces demands to address data leakage from many fronts. At the federal and state levels, there are laws in place to protect sensitive customer data. Regulated entities such as financial institutions have controls they must comply with for the protection of the personal and financial data of individuals. Organizations such as the Payment Card Industry (PCI) Security Standards Council provide a framework of security requirements to inhibit credit card data loss.

From an executive management and board perspective, there is significant reputational and financial risk in the event that sensitive data is leaked to external parties. Management is ultimately responsible for overseeing a comprehensive data leakage security strategy, which includes development, implementation and maintenance, as well as assigning responsibility for the implementation. At least once a year, management should report to the board or an appropriate committee of the board on the overall status of the information security program and the financial institution's compliance with the guidelines.

Security and risk management is not just an IT issue. It is essential that the IT risk manager, using effective communications skills, impel the appropriate IT owners and line-of-business managers to accept explicit, written responsibility for residual risk impacting the systems and processes for which they are responsible, on either a direct or a dotted-line basis. Risk managers should develop mechanisms for assignment and acceptance of residual risk and risk decisions — for example, signature forms, processes and policies that address the requirement and execution of risk acceptance. The risk manager should also develop mechanisms to convey residual risk levels that remove reference to technology but still support good risk-based decisions at a business level that may result in the implementation of technical controls.

The threat of data loss is pervasive throughout any enterprise. No matter how it happens, there is almost always a human element involved in the event. Most often, leakage is unintentional and some employees may not even be aware that their actions result in data leakage. For example, work data may be transferred to a home computer by sending files using personal email, by using a USB flash memory drive, or by going home with a business laptop. Other more deliberate leaks may result from "crimes of opportunity" due to weak controls surrounding the data. Leaks may also involve proprietary data or intellectual property loss.

At the other end of the spectrum, sensitive data loss may be the result of intentional acts by a disgruntled employee or by attackers using worms, computer exploits or social engineering techniques waged against the financial institution's staff. According to a world-wide survey commissioned and published by Cisco Systems:

- 70% of IT professionals believe the use of unauthorized programs resulted in as much as half of their companies' data loss incidents
- 44% of employees share their work devices with others, unsupervised
- 39% of IT professionals reported that they had to address employees accessing unauthorized areas of the network
- 46% of employees admitted to transferring files from the company network to their personal computers when working from home
- 18% of employees share their passwords with co-workers

Businesses may be quick to plug-up the holes their sensitive data is leaking out of with software solutions. As expected, silver-bullet solutions using various technology widgets, or poorly configured and implemented Data Leakage Prevention (DLP) appliances, may do little more than take-up rack space in the datacenter. Building a sound, risk-based strategy to manage sensitive data and implementing a framework of cross functional design controls is the key to reducing the risk of data loss.

Build a data inventory

Sensitive data cannot be protected from loss if you don't know where it resides in the organization. However, before the search for sensitive data begins, it is critical to know what to look for first. Categorizing and labeling data is an important initial step in order to separate the wheat from the chaff.

The first step is to define the proprietary data, intellectual property, sensitive customer data, health data, employee data, credit card data, etc., and then determine how averse the organization is to the loss of that data. To avoid the pitfalls of operational groups classifying data differently, each classification should be determined at a relatively high level to ensure consistency throughout the organization.

With an understanding of the types of sensitive data to look for, identify the various business processes that use the data throughout the organization. Those processes may include, but not be limited to:

- In-house applications systems
- Network infrastructure
- Electronic media
- Hardcopy media
- Third-party relationships

The next step is to perform an inventory of the various places where sensitive data resides. Include locations where data is transmitted, couriered, stored and shipped for destruction. Transmitted locations may include business partners, vendors and employee homes. Identify the processes related to recycling efforts and computer e-waste disposal of hard drives, memory, personal backup and portable storage media.

It should be noted that some of the business processes listed above have obvious interfaces to data and others may take some sleuthing to find. Understanding how each business owner and staff use sensitive data is very important to the success of the inventory collection. Discussions with business owners often reveal, for example, that the staff may be exporting sensitive information to a spreadsheet program for resorting purposes, improved formatting of the data in reports, or to aggregate information from various sources. In this example, sensitive data is transferred from secure application servers to less-secure workstations. Another effect of aggregating information from various sources such as customer information and credit card information is that it may result in the newly composited information becoming sensitive data.

As part of an effort to work collaboratively, staff may also share data using email, which inadvertently puts copies of that data on email server drives as well as the email backup tapes. Staff may also collaborate by sharing their network drive's share directory or even shared folders directly from their own hard drive. Alternatively, staff may use USB memory devices to easily share data between coworkers. Each of these scenarios can contribute to unintentional data loss. The opportunities to secure the business process and the data will be derived from understanding how the data is actually used in the organization and providing secure solutions to collaborate and manipulate the information effectively.

Threats to data

Once a comprehensive inventory of sensitive data is determined, conduct an analysis that takes into account all the plausible threats against each item that may result in data leakage. To help determine potential threats, consider the following conditions that may contribute to data leakage:

- Accidental disclosure
- Unauthorized disclosure
- Unauthorized access
- Inappropriate permissions
- Weak access controls
- Vendor controls
- Encryption
- Physical access

Other noteworthy threats to sensitive data may not be evident without security testing. Those threats may be borne from an ineffective security infrastructure, including:

- Poor controls over firewalls, routers and switches
- Vulnerabilities in the services running on network computing systems due to an unsuccessful implementation of a security patch management program
- Weak standards for user and administrative access managed by Active Directory or other directory service controls
- Weak standards for those enterprise applications with proprietary, stand-alone access control functions
- Weak standards applied to access controls for accounts in database management

Finally, evaluate the threats by considering their compliance to applicable regulatory requirements and determine if the design has inherent risks that may result in information leakage.

Determine the risk

After the threats to sensitive data are inventoried, rank them by determining the impact to the business if the identified threats are successfully exploited. The rankings can be high, medium or low, or more granular with a numbered score if complexity and size require additional detail. The ranking should also take into account any viable compensating controls that are in place and evaluate the likelihood that the threats can be exploited. The threat identification and risk assessment process is an on-going course of action that, once started, should be reviewed regularly to ensure that the protection mechanisms currently in place still meet the required objectives of inhibiting data leakage. Not performing a threat and risk analysis may result in data disclosure, disruption of service or damage. It is critical to perform a threat and risk analysis. Please refer to the Managing IT Risk through a Risk Management Framework section earlier in this document for more information on the risk assessment process as well as various risk frameworks.

Secure the data

Once the risks are ranked, a pattern of similar control weaknesses such as sharing user IDs, a lack of change management or unencrypted sensitive data may begin to emerge across different business processes. Typically, these similarities may include higher risk issues associated with access control privileges, open services or encryption. By taking an enterprise-wide approach, instead of delegating risk remediation to individual department silos, a singular, unified application of controls and compliance can be implemented for all functional groups. Utilizing an enterprise approach, the resources to implement the necessary controls for remediation are not duplicated and the methodology remains consistent.

Many causes of data loss are the result of missing or inadequate controls to secure basic technologies. Take advantage of securing those low-hanging fruit technologies in the organization, which are also likely contributors to data leakage. The following is a "usual suspects" list of security concerns that may promote data loss if effective design controls are not implemented:

- Optical and electronic media — Disable CD/DVD ROM drives and ports for USB memory and MP3 players on computer workstations.
- Wireless technologies — Tightly secure WiFi access to the network using known best-practice standards over authentication, encryption, access controls, VPN and firewalls. For smartphone technologies, apply Active Directory lockdown controls including password protection and data wiping. (For more information, please contact us for a copy of our white paper on smartphone risks.)

- Email and instant messaging — Implement anti-virus, anti-spam and malware controls. Control attachment usage or consider alternative solutions to transfer sensitive data. Aside from event logging, most messaging solutions, including Exchange, have mailbox-related monitoring disabled by default. Additional monitoring should include mailbox logins, access controls, management, configuration and moves.
- Consider the advantages of instant messaging (IM) within the organization only. If permitted by policy to use IM externally, use the existing controls already in place to secure email to also secure IM.
- Internet usage — Enforce the Internet Usage Policy. Granulate user access to the Internet. Make the patch-management of browsers a high priority. Limit off-hours access to the Internet. Limit Internet services such as remote management, administration, file transfer, peer to peer, streaming media, ICMP, DNS, webmail, Internet mail, POP3, time, etc.
- Virtual Private Networks — Monitor usage and access control events. Use standards based high encryption. Use directory service authentication for expiration and lockout controls. Consider using certificates. Granulate access to the resources on the network.
- Telecommuters — Manage laptops or desktops. Consider the advantages of thin client access to the network. Disallow shared access of the remote computer by non-employees. Control anti-virus and patch management controls. Implement whole disk encryption. Use optical and electronic media controls. Implement a clean desktop policy including shredding sensitive hardcopy data.
- Network access — Implement Penetration Testing and an external and internal security assessment programs. For in-house developed Web applications, conduct application level security reviews and application code reviews.
- Physical access — Limit building access. Review building and secure area access logs. Address tailgating, which is an intrusion technique in which an employee is followed through an open door into a secure area or building. Implement surveillance as appropriate.
- Hardcopy — Limit the physical access to sensitive hardcopy documents. Conduct "Clean Desk" after-hours audits to check for sensitive data left uncontrolled on desks, password credentials written on sticky-notes or under keyboards, sensitive info in cubicle waste bins, recycle bins and in open shred bins.
- Backup — Encrypt backup media containing sensitive data. Encrypt sensitive data transmitted to backup sites. Manage storage media not in use or being decommissioned from use and destroy the data appropriately.
- Monitoring — Conduct reviews of event logs, infrastructure device logs, access logs, firewall logs and intrusion detection logs.
- Policies — Develop and implement policies. Typical policies related to data leakage may include but not be limited to the following:
  - Data classification
  - Data labeling
  - Data management
  - Authorized/unauthorized data on mobile devices
  - Authorized/unauthorized data transferred to magnetic and optical devices
  - Encryption of data (based on classification)
  - Least privilege policy of data
  - Telecommuter management
  - Workstation usage
  - Physical access
  - Transmission of data
  - Storage and destruction of hardcopy and electronic media

Securing the data from the threats and vulnerabilities that facilitate loss is only part of the equation. The rest is to ensure the data remains secure. It needs to be defended using a monitoring, review and prevention system that inhibits unauthorized access, tampering and theft.

Defending the data

Monitoring and testing of controls are two fundamental operations to ensure that the data remains protected from leakage. Monitoring is a surveillance mechanism to detect data loss by capturing perpetrators in the act of unauthorized access or attempting the unauthorized mitigation of data. Testing is a methodology to ensure that the security controls put in place to effectively protect the data are actually working, and that the monitoring process triggers the appropriate protective measures.

Monitoring — Depending on how risk-averse the enterprise is to data loss, the monitoring of sensitive data may range from simple event logging methodologies to the sublime. The most rigorous approach would be a layered monitoring method. Similar to the Russian Matryoshka nesting dolls, this layered approach starts with monitoring the sensitive file, the folder it is in, the drive it is in, the server it is in, the network it is in, the domain it is in, and so forth. When monitoring each piece of sensitive data, the layered approach typically yields mountains of log data and is often resource intensive to review.

Another scenario to secure data is to use an interface methodology. Instead of monitoring the universe of threats, this risk-based methodology intelligently determines what "touches" or interfaces with the sensitive data and then monitors those activities. The interface method usually encompasses monitoring the threats already determined in the inventory phase described earlier. The mountain of event logs is diminished and the review of those logs can be more careful. Using automated tools to review logs based on consistent business rules reduces human error in the review process and allows the 24/7 monitoring systems to intervene and alert the appropriate staff of potential data loss events to be investigated.

Once the data is inventoried, analyzed, prioritized and secured, monitoring and prevention tools such as DLP can finally be considered as a viable solution to assist in the leakage prevention program. The prevention functionality of DLP to actively inhibit data loss events makes it an effective tool to assist and enforce certain key aspects of the data leakage program. However, DLP may be easily rendered ineffective when it is relegated to run in monitor-only mode. In fact, these solutions quickly become "non-productivity" devices because they require recurrent human intervention from IT staff to interpret threats, and clear out false positives or nuisance alarms flagged in monitor-only mode. Running DLP devices in prevention mode may initially be problematic until the business rules are adjusted to the enterprise. In the long-term, DLP should become less burdensome as the prevention process is adjusted to the environment and further automated. There are many DLP providers on the market, with each having its own approach to leakage prevention. By assessing the residual risks to the organization after implementing the data leakage program, choose the DLP solution that best complements the existing or residual risk shortfalls. It should be noted that DLP solutions typically quarantine sensitive data. These stores of quarantined, sensitive data can become a prime target for attack. As a result, DLP devices themselves must also be strictly secured and monitored.

Testing of controls – For SEC and FI regulated organizations, testing of controls is not a new concept and should already be part of the business DNA. Management may be obligated to attest that the design and operational controls protecting data from loss or theft are effective in regulated businesses. By following the guidance described previously to inventory the data, determine the design controls and evaluate the threats against the data, those organizations that choose to test controls themselves already have much of the analysis prep work completed. The balance of the process is primarily designing tests to assure that the effectiveness of the controls in place protect the data from loss. It is essential to test the implementation of the monitoring controls as well. Testing of controls should evaluate the effectiveness of the DLP system's preventative capabilities and alerting system. Alerts generated by event logging controls such as hardware, storage, Internet and access permissions misuse should also be assessed. Monitoring controls have broken designs if alerts are not generated, not reviewed, not reported to management, not retained and if not resolved. Alternatively, some organizations may seek the expertise or independent evaluation of external resources to conduct the testing of controls to assure the effectiveness of their data leakage controls.

Management solution

Sensitive data is dispersed throughout the enterprise, which easily facilitates its leakage outside of the organization. If the strategy to protect data from leakage is the application of traditional methods and approaches to secure data from loss such as conducting vulnerability and penetration tests, there is a likely disconnect between the threats the organization is prepared for, and the threats that are most likely to take place. Management should implement a complete solution to address its data leakage concerns. Designing an enterprise-wide and risk-based security framework of business processes and automated tools to identify, secure, monitor, test and defend sensitive data from loss is a better investment than entrusting the data solely to security widgets and data leakage appliances.

Cloud computing

What is cloud computing?

The term "cloud computing" evokes images of cutting edge start-up technology companies, with the whiz-kid CEO, sandaled software developers and a foosball table in the conference room. However, increasingly, mainstream organizations are diving into the world of cloud computing and surprisingly, can look to the conservative financial industry as an early adopter of the service.

First it's important to define cloud computing. It should be noted that cloud computing is computing model, not a technology. In the cloud computing model, all the servers, networks, applications and other elements related to data centers are made available to IT and end users via the Internet, in a way that allows the organization to purchase only the type and amount of computing services that they need. There are three basic types of cloud computing:

- Software as a Service (SaaS): The most widely known and widely used form of cloud computing, SaaS provides all the functions of a sophisticated traditional application, but through a Web browser, or a small locally-installed application.

  SaaS eliminates worries about managing application servers, application development, software patch management, data backup and other IT operational issues associated with managing an enterprise application. High profile examples in the news today include Salesforce.com, ADP Payroll Services and VoIP from Vonage. Functionally, this is similar to the service bureau model offered by every major financial industry core system provider for decades. While in the past, financial institutions had dedicated network connections to these vendors, encrypted Internet connections are being offered as a cheaper alternative.

- Infrastructure as a Service: Provides grids or clusters or virtualized servers, networks, storage and systems software designed to augment or replace the functions of an entire data center. The highest-profile example is Amazon's Elastic Compute Cloud (EC2) and Simple Storage Service, but IBM and other traditional IT vendors are also offering services, as is telecom-and-more provider Verizon Business. While not widely adopted as the core system service bureau in the financial industry, it is common to see financial institutions outsourcing their Internet and security infrastructure to a vendor who can manage and monitor this infrastructure on behalf of the institution.
- Platform as a Service: Provides virtualized servers on which users can run existing applications or develop new ones without having to maintain the operating systems, server hardware, load balancing or computing capacity. Highest-profile examples include Microsoft's Azure and Salesforce.com's Force.com. This has a low rate of adoption in the financial industry and is only seen in the largest of institutions.

Growth of cloud computing usage

There is a widely held belief in the IT industry that cloud computing will be widely adopted over the next five years. In fact, Gartner predicts that by 2012, 20 percent of businesses will own virtually no IT assets. Increasingly in the financial industry, depositories that had not hosted their own core banking systems are considering service bureau options as a viable alternative to an internally hosted system. However, having a hosted solution may just be the first step. If you're going to have your data and applications hosted externally do you really gain a competitive edge with the way you perform item processing, or should you find a vendor that will host the application, the associated infrastructure and process the documents for you?

IBM Global Services and HP are serving up more and more "x-as-a-service" items on their menus, from infrastructure to storage. Infosys is offering end-to-end IT and business processes — Source-to-Pay for procurement, Hire-to-Retire for HR — on a pay-per-use basis built on a cloud backbone. Wipro Technologies is piloting a central computing cloud to study the potential of the trend. Patni Computing Systems is selling a "cloud acceleration service" to help developers migrate their processes to a cloud-based model the way it did internally and is experimenting with testing-as-a-service.

However, the belief in the growth of cloud computing is not without skeptics. Larry Ellison, CEO of Oracle, dismisses the term cloud computing as a new definition of services that have been offered by software vendors for years. And the skepticism is also at the department level of many companies' IT operations. In the 2010 ISACA IT Risk/Reward Barometer survey of over 1800 IT professionals in the U.S., only 10 percent plan to use cloud computing for mission-critical IT services. While another 15 percent plan to use it for low-risk IT services, a whopping 75 percent either do not plan on using cloud computing services or are undecided of its adoption in their organization. Based on these stats, Gartner's 20 percent forecast may be optimistic.

Benefits of cloud computing

The proponents of cloud computing are quick to point out their benefits, the primary being lower costs. These cost savings can be in various areas, including:

- Reduced data center costs: Managing an enterprise data center is an expensive proposition for an organization running a mission critical application. In the financial industry, regulatory requirements around business continuity and environmental protection leave financial institutions with little choice but to invest heavily in environmental and physical security controls that may never be used. Cloud computing vendors can leverage their data facilities over many customers who can then pay a fraction of the overall cost of maintaining an enterprise data center.
- Minimize IT operations duties: With fewer servers or network equipment to support, IT operational duties will be reduced, resulting in a smaller IT staff, which could result in substantial savings.
- Lower maintenance costs: While organizations often have the capital costs of hardware and software up front, there are yearly maintenance costs for hardware and software support. A cloud computing vendor can spread these costs over many customers, therefore, lowering the costs for all.
- Improved cash flow: In the current economic times, many financial institutions are struggling with cash flow. By converting an upfront capital expenditure to a lower monthly subscription cost, organizations can conserve valuable cash in the near term.

There are benefits to the organization beyond cost. Decreasing the operational duties of the IT staff can free them up to think more strategically about how the infrastructure could support the business needs of the organization. They can also spend more time monitoring and responding to operational issues and leave the daily mundane tasks to the cloud computing vendor.

Cloud computing is often very scalable. This is a time of opportunity for many financial institutions that have been able to increase asset size quickly by purchasing competitors that are suffering financial hardship. By having an outsourced infrastructure, scaling up to handle the additional capacity is often just a question of cost, with minimal or no effort on the part of the IT staff. However, increasing the capacity of an internal IT infrastructure could be highly costly, not to mention time intensive.

Reduced downtime is also a major benefit. Cloud computing companies invest in large, redundant IT infrastructures that are geographically distributed. They can also leverage unused hardware to provide clustering and failover capabilities. Premier cloud computing companies often invest in IT staff that is not only experienced with technology, but also possesses knowledge of best practice IT operational methodologies around change management, a lack of which is a primary cause of downtime for internally managed systems.

Risks of cloud computing

With the acknowledged benefits of cloud computing, it is understandable why it is being promoted as the IT computing model of the future. However, like any new models, there are risks to consider.

Security risks

The business risk in the adoption of cloud computing is security. In fact, while the usage of cloud computing has increased, there has also been a corresponding increase in cyber attacks, including penetration of corporate networks. These security issues can be broken down into the following areas:

- Protection of data: In a cloud computing environment, an organization is giving up control over its most valuable asset — information. While most organizations focus on the secure communication method with cloud computing vendors, surprisingly, in many cases, organizations are not even aware of their vendor's security controls over the storage of that data. In the Ponemon Institute's 2010 Access Governance Trends Survey, only 17 percent of companies with data hosted by external providers were able to verify that confidential data was encrypted in their vendors' database. There is also a noticeable lack of common data handling and security standards in the cloud computing environment, including rules that would require vendors to disclose where data is physically stored, increasing the risk that data is housed in countries not bound by U.S. or European data security laws.
- Security access procedures: Cloud computing has also led to the decentralization of access controls to the business units beyond IT. In the Ponemon survey, 73 percent of respondents said adoption of cloud-based applications is enabling business users to circumvent existing access policies.

  Many times, cloud-based services are purchased directly by the business units, especially for SaaS offerings. These purchases can be made without the consideration of user access management. Increasingly, people in the business units, rather than the IT department, have growing influence over granting user access to information resources. Prime examples are the use of Salesforce.com by sales departments or ADP by payroll departments.
- Security governance: Regulators expect strict security policies to be adopted by financial institutions. These policies can cover a wide range of areas from guidance around employee background checks to management of confidential information. However, there is no guarantee that a cloud computing service provider has implemented a strict level of IT security governance, despite the fact that they may hold and process critical client information.

Monitoring risks

Outsourcing an application or infrastructure to a cloud computing vendor will leave organizations at the mercy of the vendor to report security or operational issues. Other than the direct access to the outsourced service, organizations have no access to the vendor's infrastructure. In some cases, cloud computing vendors don't offer any proactive monitoring communication at all, leaving organizations to wonder about the performance of the infrastructure. Cloud computing vendors rarely allow third party vendors to independently monitor their systems, so any information you receive would be through the viewpoint of the cloud computing vendor.

Contractual and cost risks

Another major risk in cloud computing is the lack of attention to the contractual terms in a cloud computing agreement. Organizations often sign contracts with cloud computing vendors that lack basic operational and security components such the following:

- Clear definition of availability of service: A vendor may define availability as the ability to access the software. However, if the access is too slow for practical usage, can that truly be defined as an available system?
- Guarantees on availability of service: Organizations that choose vendors across time zones or international borders risk that systems may be down for maintenance during critical business hours.
- Financial redress in the event of failure: Service that is unavailable or unusable could be devastating to an organization's financial situation. However, cloud computing service providers often limit their liability, even for disruptions that they have caused internally.
- Service level agreements (SLA): Many cloud computing contracts offer no service level agreements or poorly written SLAs. Additionally, contracts may not include guarantees of the correction of issues if an SLA is not being met.
- Cost: While there are many cost benefits of outsourcing services to a cloud computing vendor, if usage is not monitored, the cost benefit could evaporate. While the capital costs of building the infrastructure is lowered, once the financial institution reaches a critical mass of usage, the costs of providing network bandwidth increase to a point that it is more cost effective to build the infrastructure internally.

Risk mitigation steps

The risks to using a cloud computing vendor are daunting, but can be mitigated by implementing a series of controls. These controls should be included in a financial institution's technology service provider program and cover the following areas.

Strategic planning

Before organizations move to a cloud computing environment, a clear articulation of their plan should be documented. Just stating that the organization plans to embrace cloud services in conjunction with your traditional IT outsourcing model is not enough. Ask some hard questions about where the organization needs to be over the next 3-to-5 years regarding technology. Some questions to contemplate include:

- Can you afford to maintain a data center?
- Is that custom application truly a competitive differentiator?
- How should your outsourcing strategy shift to ensure long-term value?
- Will a vendor be able to meet your data security concerns?
- Does it make sense to outsource a critical function? Alternatively, perhaps a new service that is non-critical to the organization?

Financial institutions should also clearly define the role of IT and the business units for all potential cloud computing services. These services force a greater collaboration between business units and the IT department, as well as internal audit and compliance. Pre-planning will help ensure key control areas such as access-control governance are defined prior to the implementation of new services.

Vendor due diligence

An outsourced relationship vendor, especially for a critical system, should not be approached lightly. Any potential cloud computing vendor should go through an extensive vetting process prior to selection. The following information should be carefully reviewed for any potential vendor:

- Financial condition: A cloud computing vendor in poor financial condition could be a troublesome partner. Cloud computing vendors are investing in the capital intensive IT infrastructure that financial institutions are outsourcing. So it is important that financial institutions review the financial health of their potential cloud computing vendor to ensure those investments can continue.
- Independent controls testing: A SAS 70 report is commonly obtained by financial institutions to verify the effectiveness of controls at an outsourced vendor. However, just obtaining a SAS 70 report is not enough. The report should be carefully reviewed to verify that controls that are critical to the financial institution's needs are documented. Does the report cover employee background checks? If the provider will hold financial institution data, does the report describe and test controls around database security and access? Financial institutions can request information beyond the SAS 70 report, such as test results for business continuity or penetration testing results. The financial institution has every right to expect and demand that their service providers implement the same controls that the institution itself would implement if the service was internal. Controls to review may include, but are not limited to the following:
  - Authentication controls
  - Data protection controls
  - Software development life cycle and change management controls
  - Patch management controls
  - Employee screening controls
  - Network and application monitoring controls

Review of contract terms

Financial institutions should carefully review vendor contracts to ensure they include terms that are fair and understood by both the institution and the vendor. Elements to review in the contract include:

- Precise definitions: Phrases such as "availability" and "business hours" should be defined in a way that removes ambiguity. For example, "availability" for a SaaS service should include not only the fact that the application is available for usage, but also the acceptable response time for practical usage. "Business hours" should include not only the customer's expected time of operations, but also the time zone for these hours.
- Service level agreements: If contracts do not include SLAs, they should. Cloud computing vendors should commit to defined parameters for service responsiveness and availability. These SLAs would be the basis for the financial cost of the service. If service levels are not met, customers should verify that financial penalties can be implemented that would mitigate any losses to the organization for an unavailable service or application.
- Security requirements: If confidential data is to be held or processed, organizations should include the security requirements their cloud computing vendors should implement. This could include data storage controls, human resource policies, encryption controls, etc. The vendor is serving as an extension of the financial institution's network and requesting them to adhere to the same controls is well with your right.

Conclusion

For financial institutions, cloud computing is not a futuristic technology. In many cases, financial institutions are already struggling with its adoption. Like any other operational model, the risks for the implementation of these services should be defined, assessed and mitigated. By doing so, financial institutions can benefit from the innovations from cloud computing, while still meeting their regulatory and data security requirements.

Virtualization of servers

An emerging technology gaining popularity with financial institutions is server virtualization. Loosely defined, server virtualization is using one physical server to host several virtual servers. To users on the financial institution's network, the virtual servers appear the same as real physical servers.

The hardware needed to host the virtual servers is not vendor specific but is configured with more hardware resources than a typical stand-alone server. General hardware specifications would include:

- At least two and up to 16 processors
- The memory requirements for the host operating system and additional memory for each virtual server
- Two or more Ethernet controllers
- Fast SCSI disk drives or fiber channel

The required software includes the virtual server software and licenses (Microsoft, Unix, Linux, etc.) plus the host operating system that creates the virtual environments for the virtual servers. There are several host operating system options; the following is not an exhaustive list but represents the most popular options:

- VMware from VMware/EMC
- Hyper-V from Microsoft
- Virtual Box (Open Source)

There are many advantages to implementing virtual servers in a network to replace stand-alone servers. These advantages have led to the relatively rapid and large-scale utilization of this technology as compared to the slower adoption of VOIP for example. A short list of the major advantages of virtual servers includes the following:

- More effective use of hardware resources
- Fast and efficient backup and deployment
- Faster recovery for disaster recovery and business continuity support
- Power savings and space savings due to fewer physical servers
- Provides for the testing of upgrades, new versions and new configurations in a test environment as virtual test servers can be created without acquiring separate test hardware

The advantages do not come without disadvantages that need to be managed to ensure that the financial institution does not expose itself to unneeded risk. The potential for risks, specifically security risks associated with a virtual server environment come about primarily because there are some unique variables in the environment that do not exist in a traditional network. Due to the potential for risks in a virtual server environment, we recommend that the normal IT audit include an audit of the virtual server environment itself.

Below is a list of five major security risks we have discovered in virtual server environments.

1. Virtual server sprawl
   a. Risk: Due to the ease with which new servers can be deployed it often leads to too many deployments. It is important to remember that each virtual server carries with it a certain amount of increased risk to the network.
   b. Remediation: Require that new virtual servers go through the same formal request process that physical servers go through (business analysis, IT risk impact, etc.).
2. Isolation across network segments
   a. Risk: Virtual servers located on the same physical host "share" the same physical network interface card (NIC). This may create performance issues as well as security issues as network traffic is unfiltered between the servers (application to database server(s) for example).
   b. Remediation: During provisioning, consider whether applications and virtual servers should be spread among the physical hosts to provide for more isolation (not sharing same NIC card). Furthermore, consider implementing VLANs to protect servers from the rest of the data network.
3. Server implementation processes
   a. Risk: Virtual servers may not be implemented using the same processes that a physical server might be subjected to. Examples of standard implementation processes include removing unneeded services, removing default shares, patching, etc.
   b. Remediation: Virtual servers should go through the same formal implementation processes that "real" physical servers are subjected to ensure that all virtual servers meet security baselines.
4. Security tools
   a. Risk: Security tools (testing and monitoring) are performed at the physical host level only, meaning the virtual servers may not be monitored as closely as they should (or would be if they were "real").
   b. Remediation: Use the same toolset for each of the virtual servers as you would for the physical servers. Examples include log monitoring, event monitoring, etc. Just because they are virtual servers does not mean they need less monitoring and support; only the hardware goes away.
5. Patching and Maintenance
   a. Risk: Virtual servers sometimes tend to be forgotten because they can't be seen hanging in the equipment rack. We've noticed that the "forgotten" virtual servers tend to be the specialized application servers such as database servers for a particulate application, application gateways, etc.
   b. Remediation: Just like the physical server, virtual servers need to be maintained and patched. Similar to No. 3 above, even though the hardware is gone, the virtual servers need to be patched.

Web-based application security

The Web browser Mosaic was released by the National Center for Supercomputing Applications (NCSA) at the University of Illinois Champaign – Urbana back in 1993, starting the wide-spread use of Web-based or browser-enabled applications. During the past 17 years, Web applications have come a long way from early simple "brochure" sites to full-fledged applications that rival the features of traditional "non-Web" applications. As Web-based applications have become more complex and feature-rich, there is the potential for more and more security vulnerabilities within the applications.

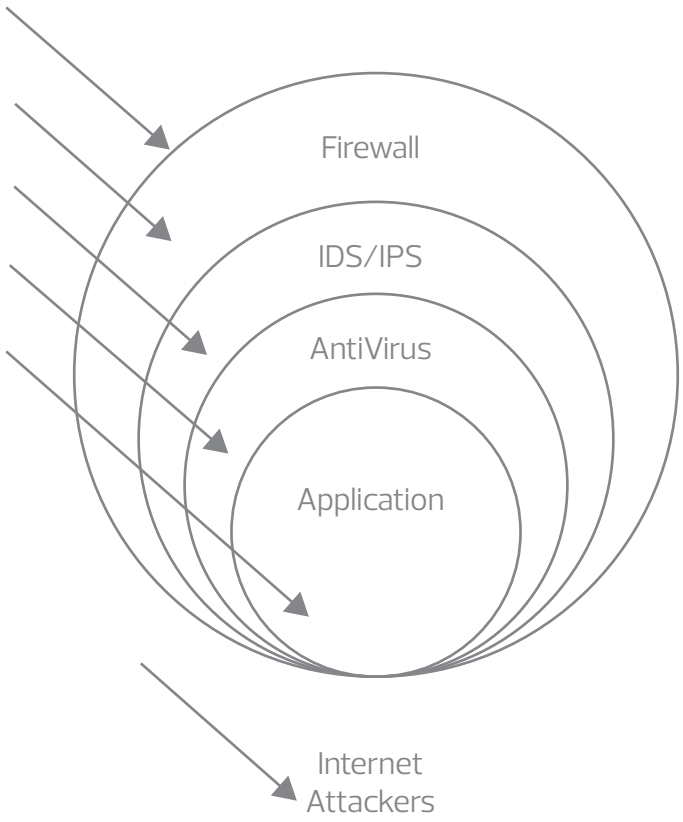
Financial institutions have traditionally treated the Internet Banking application as the only Web-based application offered by most institutions. There are exceptions such as the occasional Trust system and e-statement systems but by and large, if a financial institution's management is asked for a list of their Web-based applications, they will think only of their Internet Banking application. What is frequently overlooked is the financial institution's website, which over time has often morphed into an application itself. Examples of application functionality we've found on financial institution websites are:

- A link so that customers can sign up for a newsletter
- A functional "buy/sell/trade" application similar to a localized "Craigslist"
- Website customization features so that users can have the website look the way they want it to look or highlight services that are most important to them
- A link so that they can be notified when the website gets updated

In traditional system development processes, the functionality of the application in meeting the business needs is most often the primary driver of the development process. Web-based applications may be submitted to the same traditional system development processes to ensure that business needs are met, but they have an additional security requirements process that often appears to be overlooked. There should also be security testing of the application prior to putting it into production. Remember, a Web-based application is exposed to the entire Internet, NOT just a limited set of users as a traditional application would be.

Web-based applications often also have the added requirement of meeting marketing requirements that may add additional complexities to the application above the functionality requirements. While there is no general rule of thumb or heuristic that we've seen, in general most developers would agree that additional complexity potentially adds additional risks.

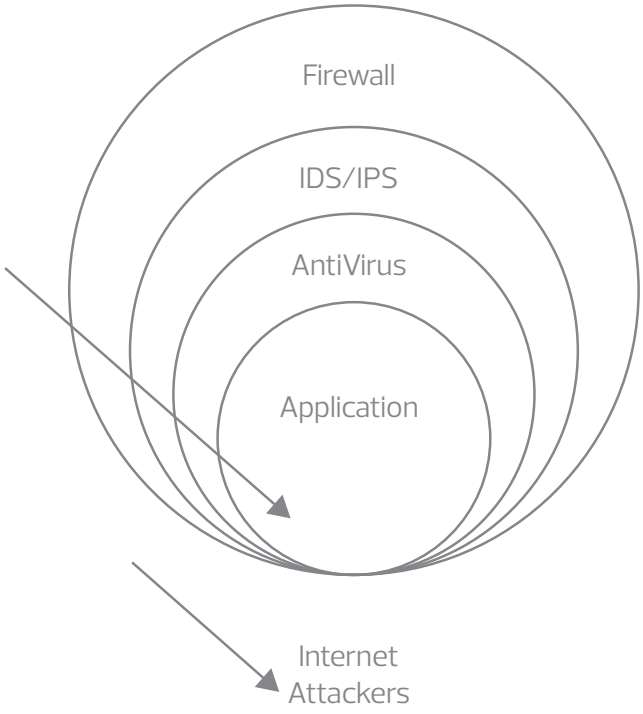
There appears to be a common misconception in the IT field that an application server is adequately protected by a firewall, intrusion protection system (IPS) or antivirus. These items do make up the common "layers" used to protect other information assets that may be exposed to the internet (mail servers, for example). The following graphic indicates the view of layers to protect an asset (application). The arrows represent the attacks and the misconception that the attacks have to work through various layers to get through to the application.



The issue with the graphic at the left is that if the application is not developed with good security, the layers do not help secure the application itself. The following graphic illustrates that an attacker can directly access the application and that essentially, only the application's security features can protect it from an application attack. Why would an attacker be able to bypass the layers of protection? An attacker can bypass the layers because:

- The firewall has to permit the attacker traffic, as legitimate traffic has access to the application (normally TCP ports 80 and 443).
- The IDS/IPS normally will pass the traffic as well, unless the attacker triggers a signature that sets the IDS/IPS to block the traffic.
- The antivirus on the application server is also unlikely to detect issues with the traffic and if the attacker executes code on the server as a part of the attack, in most cases the execution is permitted.

As illustrated below, Web-based applications are exposed to unique security risks compared to other Internet exposed systems. Below are some common Web-based application risks that may help explain the specific risks to applications in more detail:



1. Injection (URL, SQL, etc.)
   a. Risk: Injecting commands into an application so that the application is tricked into executing the commands. The impact is normally severe in that the attacker gains access into the underlying database and operating system itself; normally as administrator equivalent.
   b. Remediation: Require that the application require input validation (example: numbers only permitted in a "phone number" field). Also consider minimizing access rights to the database from the application.

2. Cross-site scripting (XSS)
   a. Risk: Raw data from an attacker is sent to an innocent user's (customers) browser, typically permitting them to steal sensitive user data or redirecting the customer to a bad site.
   b. Remediation: Develop the application so that it does not include user-supplied input to the output page. Also consider encoding ALL user-supplied input.

3. Authentication and session management
   a. Risk: Because of the way a Web application works, authentication and session management have to constantly be passed from client to server. If this communication is not secured, user accounts can be compromised.
   b. Remediation: It is essential to secure this communication. Be sure to use SSL to protect the credentials and to encrypt the session ID information.

4. Insecure direct object references
   a. Risk: An application needs to reference certain data sets (if I am logging into my Internet banking account, I need to have the application at minimum contact the account database so my account information can be accessed and displayed in my browser). When the information is displayed, it should not show direct object reference information. Attackers will be able to access unauthorized files or data.
   b. Remediation: Ensure that your application does not show direct reference mapping in the output.

5. Security misconfiguration
   a. Risk: Applications rely on secured platforms. Operating system, network and development tools and development practices all need to be secure or the risk of backdoors being installed on the system increases.
   b. Remediation: Follow standard system hardening techniques for all systems supporting the Web-based application. Also ensure that the systems are patched.

The topic of Web-based application security is complex and can be confusing. As a takeaway from this discussion we've summed up the following important items:

- Most financial institution websites have become more application-like.
- System development for Web applications MUST contain a security design component in the initiation stage and throughout the development process.
- The application should be tested prior to going into production and thereafter either annually or whenever a significant change has been made.

Our Authors

Hussain Hasan is a Principal with the Technology Risk Advisory Services group. He specializes in enterprise risk management (ERM), Sarbanes-Oxley (SOX), strategic planning and information technology (IT) security. Hussain has over 20 years of experience in various capacities and industries, especially in specialized audit and consulting in both internal audit and public accounting settings. Hussain is currently a member of the Institute of Internal Auditor's Advanced Technology Committee. Hussain can be reached at +1 847 413 6287 or at hussain.hasan@rsmus.com.

Doug Underwood is a Principal in RSM's Technology Risk Advisory Services. Doug has over 18 years of experience providing IT controls and security services to the financial institution industry. Prior to joining RSM, Doug was a Bank Examiner with the Comptroller of the Currency. Doug can be reached at +1 612 376 9210 or at doug.underwood@rsmus.com.

Loras Even is a Principal with the Technology Risk Advisory Services group in the Waterloo, Iowa, office. He brings more than 28 years of experience in information technology, which includes 11 years of focusing on security. Loras specializes in network security assessments for regulated clients. Loras has directed the security assessment practice for a variety of industries, including financial institutions, health services, manufacturing and government. Loras can be reached at +1 319 274 8541 or at loras.even@rsmus.com.

Sudhir Kondisetty is a Principal in the RSM Technology Risk Advisory Services group. Sudhir specializes in information technology (IT) security risk assessment, IT general controls review, network infrastructure security testing, Sarbanes-Oxley IT reviews, SAS 70 and IT project management. Sudhir has over 20 years of IT experience in various industries. Sudhir can be reached at +1 215 648 3121 or at sudhir.kondisetty@rsmus.com.

+1 800 274 3978
www.rsmus.com

wp_fi_1015_information_technology_risk_mgmt

RSM