The Dual Security Challenge of the Information Age

The Internet was designed to share information, not to protect it.
— From an editorial by cyber security experts Jacques Gansler and William Lucyshyn*

Advances in technology have transformed the global marketplace at a dizzying speed, creating a landscape no one imagined only a decade ago. Instant and efficient electronic transactions are now an expectation rather than a convenience, and the Internet has become an essential component of twenty-first century commerce and communication. However, the same technologies that fuel our economic growth have created areas of vulnerability that threaten the integrity, availability and confidentiality of enterprise information and customer transactions.

It takes only one serious breach in a company’s information security system to damage a corporate brand and erode customer confidence. To prevent this, a zone of protection must be robust and tightly integrated wherever information enters, exits or resides. Just as important, reliable safeguards must be in place at both the enterprise and product levels to ensure that sensitive data is safe from compromise, regardless of its content, media or channel. In addition, processes and protocols must be implemented systemwide to enable a quick and effective response to any successful attack.

Industry experts suggest that enterprises use the following approach to most effectively defend against ongoing and changing threats:

- Become aware of the type and nature of cyber threats, including where and how they most often originate.
- Insist on a vigorous security policy and information risk mitigation strategy. In conjunction, adopt state-of-the-art technology to identify and shore up potential security vulnerability.
- Maintain an ongoing program of security education for employees and customers.

Risks to the Enterprise

Large enterprises today have complex technology infrastructures that process and manage information resources. In the financial services industry, much of this information relates directly to customer finances (e.g., bank accounts, credit card numbers and transactions). An essential component of an enterprise is a security program that will protect all data (including customer data) from unauthorized access.

Information can take numerous routes on its way into and out of an enterprise, making it imperative to protect against both internal and external threats. Studies indicate that insiders commit approximately 80% of all corporate security breaches. And while a great deal of attention is paid to online security breaches, cyber crimes are committed using a wide range of networks, including hard-wired and wireless computer and telephone networks—all of which can be hacked. The consequences of these break-ins range from theft of confidential data to major disruption of network systems.

Hackers specialize in breaking into computer networks to gain access to corporate, government and private information resources. They are generally (but not always) external to an enterprise. Hackers take advantage of every channel linked to a company’s network to crack user passwords or enter vulnerable systems. While they once hacked for the short-lived fame, they now do it increasingly for fortune, harvesting the private information of vast numbers of consumers and then selling the information.

Viruses, a common tool of hackers, are infectious forms of malicious software (sometimes referred to as “malware”) that sometimes download into vulnerable computers. Viruses perform various actions ranging from simple nuisances to deletion of user data, with self-replicate. Macro viruses become embedded in the macro commands of popular spreadsheet programs like Microsoft® Excel®. A recent study by CFO Research Services showed that 73% of small to mid-size companies rely on spreadsheets that become susceptible to macro viruses when financial and budgeting statements generated by those spreadsheets are exchanged via e-mail.

Forrester Research reports that in October 2006, the Haxdoor virus, which was prevalent in Great Britain, robbed 8,500 users of key e-mail and search engine data from a single server. Other widespread virus attacks have included features that allow a virus to download a new version of itself every 30 seconds, creating unpredictable mutations that defy the best efforts of virus trackers and researchers.

In addition to breaching hardware and software systems, more than 75% of corporate intellectual property is stored in e-mail, according to Massachusetts-based Enterprise Strategy Group, a leading industry analyst firm. E-mail that is unchecked by strong virus protection poses an enormous risk to corporate data, as it can spread mutating viruses throughout a company quickly and without detection.

Trojan horses, programs that “unpack” a malicious program (possibly once an e-mail is opened or when a program is installed), are also valued by hackers. Trojan horses may appear to be useful or interesting programs (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. There are two common types of Trojan horses. One is otherwise useful software that has been corrupted with malicious code that executes while the program is used. Examples include weather alerting programs, computer clock setting software and peer-to peer file-sharing utilities. The other type is a standalone program that masquerades as something else, like a game or image file, in order to trick the user into installing the malicious program.

The Growing Need for Awareness as a Strategy

According to the 2006 CSI/FBI Computer Crime and Security Survey:

• Nearly 75% of respondents said that the key areas of security awareness needing focus were security policies, network security and security management.

• Respondents from 10 of the 15 business sectors polled said they didn’t think their organizations spent enough on security awareness.

• The chief concerns in the near term are data protection and application software security.
Phishing (pronounced “fishing”) is the use of legitimate looking e-mail to lure individuals to fake Web sites, where they are asked to disclose confidential financial and personal information, like passwords, credit card account numbers or social security numbers. The information is then used to gain access to the user’s accounts. The most common type of phish is an e-mail threatening account closure if the recipient does not immediately log in and take action.

Distributed Denial of Service (DDoS) is one of the most popular of Web application attacks. DDoS overwheels servers with bogus traffic, tying up resources until the system is at a standstill, effectively preventing anyone from transacting business using that Web site. The aim of such an attack is to find a security loophole or flood the application with requests until it becomes overloaded and shuts down.

Spoofing is an electronic impersonation of an Internet Service Provider address. Intruders use spoofing to hop through the Web application network, exploiting machines that have established trust-based relationships with each other. Their attacks are increasingly well targeted, zeroing in on handpicked companies, divisions within corporations, and specific people, finding out the interests of employees via chat rooms and newsgroups. Their ability to adapt to different types of security defense mechanisms has made them an ongoing threat to sensitive enterprise information.

The First Lines of Enterprise Defense

Strong and reliable information security begins at the enterprise level with basic firewall and antivirus protection, as well as three critical components sometimes referred to as “The Three A’s”: authentication of individual identity, authorization of permissions and stringent auditing of enterprise data, data traffic, processes and protocols.

Antivirus software searches servers, hard drives, stored digital files and e-mail attachments for known or potential viruses by checking for certain patterns of binary code, against a stored virus definition file. When a new virus comes out, the virus definition file needs to be updated to include the new virus pattern. The importance of keeping definition files updated cannot be overstated; antivirus software without updated definition files is useless. Most good antivirus software will automatically update definition files (or at least have the option to do so). In addition to using state-of-the-art technology to block viruses, a company’s employees should be educated to be mindful of suspicious-looking e-mail solicitations. They should also be trained to avoid responding to any spam messages, or opening e-mail attachments where there is no clear business relevance, since the attachment may contain a virus.

Firewalls are a critical element of protection for a network of any size, protecting all entry and exit points of the network. Firewalls may exist either at the network perimeter or as partitions within the enterprise intranet. Firewalls provide barriers that protect against hackers who attempt to break into the enterprise network and deposit viruses, Trojan Horses or other malware. Properly managed perimeter defense can thwart denial-of-service attacks.

Authentication is the process of verifying the digital identity of the sender of a communication, such as a request to log in. The sender being authenticated may be a person using a computer, a computer itself or a computer program. Authentication is a primary defense against spoofing and other forms of attack. Hackers that are kept at bay cannot corrupt a network or applications. In addition to using state-of-the-art technology to block viruses, a company’s employees should be educated to be mindful of suspicious-looking e-mail solicitations that seek to gather security information from the user.

Forrester Research reports that in October, 2006, the Haxdoor virus, which was prevalent in Great Britain, robbed 8,500 users of key e-mail and search engine data from a single server.
**Multifactor authentication** is the preferred method to prevent hackers from cracking passwords in defeat user authentication. Instead of relying on predictable passwords or a person’s user name as the sole means of defense, multifactor authentication requires an additional type of authentication, such as *something you know* (for instance, a password or PIN) and *something you have* (such as a piece of hardware or software that uniquely identifies the individual). To be effective, multifactor authentication needs to be user-friendly or it defeats its own purpose. If users find it burdensome to use every time they need to access the system, they may resort to shortcuts that end up compromising their security, like writing their password on notes that are taped to their computers.

**Authorization**, also referred to as “access control,” is the process of confirming that a person whose identity has been authenticated has permission to access certain information or perform specific operations. Authorization can be conducted in many different ways, but is generally performed after a person has been authenticated. Authorization ensures that customers, insiders and administrators have limits to the information they can access, so they do not access inappropriate information.

**Auditing and intrusion detection** is the process of monitoring the network infrastructure at the enterprise and network perimeter levels and the recording of potential issues. This helps to ensure information, hardware and application security, optimal network speed and data integrity and ongoing compliance with licensing and legislative mandates. If an outside auditor is selected to perform security audits and implement security processes, due diligence must be conducted to ensure that these auditors are reliable and experienced. A company that carries out such testing should be detailed in its approach, using written documentation to cover each testing step. They should also allow a company representative to be on-site for testing, show proof of liability insurance, and be willing to sign a nondisclosure agreement. Other general measures to be observed when using outside testing vendors include conducting employee background checks for those with responsibility for or access to customer information, regular testing of key controls, creating response programs that specify the actions to be taken when security is breached, encryption of electronic customer information and establishing access controls on customer information systems.

**Other Measures of Enterprise Protection**

In addition to basic information security measures, other, more stringent elective measures are often used to mitigate the risk of the compromise of enterprise information and systems.

**Penetration testing** is a popular way to substantiate the susceptibility of an organization to attacks. Penetration testing identifies security vulnerabilities and evaluates the amount of risk that information assets are exposed to by simulating an attack on the various processes and applications of an application. Penetration tests are performed by teams other than the developers or standard users of the application.

**Implementation of Uniform Resource Locator (URL) filters** can counteract spoofing by blocking access to sites harboring harmful code, spyware, worms, Trojan horse software, etc. URL filters can also help eliminate the use of Web resources that allow files into a network without the proper virus scanning. These filters require access to the Internet via a proxy server, which is a single point for monitoring and controlling outbound traffic.

**Limiting application services** in order to minimize exposure is a strategy to consider at the enterprise level. In general, the more applications on a server, the greater the risk of attack. With fewer services available, there are fewer vulnerabilities for intruders to exploit. Companies can reduce the risk of attack by separating critical components of the infrastructure so that each server hosts only one critical service. Doing so also enables more flexible implementation of security layers that provide the appropriate level of protection when reducing overall impact, should an application attack be successful.
Information Threats at the Product Level

Lapses in security at the border of the enterprise do more than put information and systems at risk. Once intruders get in, the actual products and services offered by the enterprise can also be compromised.

Unsecured e-mail not only provides a conduit for destructive viruses that can attack product applications and data caches, it can also expose the sender’s or recipient’s personal data—Social Security Number, account or PIN information and so forth—to unauthorized entities, opening the door to financial and identity theft.

Payment fraud is one of the most significant consequences of security breaches at the product level. In online and electronic transactions (such as debit card or ATM transactions), payment fraud may be enabled when a user’s authentication credentials are stolen. Unfortunately, many individuals make it easy for hackers to crack passwords. Results of a Nucleus Research study released in October 2006 indicated that of the 325 users surveyed, one in three neglected to keep passwords confidential. Of those who keep records of their passwords, two-thirds store it in a text file on a PC or mobile device or keep it in their wallet, creating additional vulnerabilities. As a result, new government mandates in the United States and other countries require multifactor authentication or layered security in their Internet payment products.

Check fraud, a subset of payment fraud, is also widespread and broad-based. A February 2006 survey of finance and treasury managers by the Association for Financial Professionals concluded that check fraud in 2005 affected organizations of all sizes. Whether it took the form of forgery, counterfeiting, alterations, paperhanging or check kiting, an alarming 94% of the organizations surveyed were victimized. The study concluded that while most companies had adopted basic internal fraud controls, less than half have additional defenses in place such as reconciling checking accounts on a daily basis, establishing separate accounts for checks and electronic payments, and placing a “post no checks” restriction on electronic payment accounts.

Countermeasures at the Product Level

As cyber criminals become more cunning and use increasingly inventive methods to try to avoid their malware being detected, organizations will look to single vendors with cross-threat expertise and consolidated product solutions to protect their systems, their data and their business continuity.


Ongoing communication remains one of the more effective ways to comply with a security policy. Portals and e-mails that send directed messages from the financial institution to the customer are effective.
means of communication. This is a simple concept, but in today’s age of information overload, it’s easy for busy individuals to forget specific points of security protocol, or to underestimate the ongoing threat. Companies must continually remind their employees and customers to keep their passwords private and unavailable, to be wary of unsolicited e-mails or suspicious URL links, and to avoid responding to spam messages or opening e-mail attachments where there is no clear business relevance. If a company has specific information security measures in place—such as proof within e-mails that they know the recipient’s name and place of employment (hackers do not know the identity of their victims), or unambiguous URL links that confirm the company as the sender of the e-mail—those measures should be communicated clearly and reinforced at regular intervals.

**ACH services and protocols** can go a long way toward mitigating the risk of payment fraud. Of the organizations that suffered check fraud in 2005, 81% suffered no financial losses as a result of the attempted fraud, in most cases because the organization used positive pay or reverse positive pay antifraud measures for verifying whether checks presented for payment can be cashed. Twenty-eight percent of all respondents were victims of ACH fraud resulting in financial loss, attributable to the fact that those organizations failed to use ACH debit blocks or filters, and/or account reconciliation. Other methods for minimizing payment fraud include the separation of disbursement and reconciliation duties, controlled access to payment processing, daily reconciliation of checking accounts and defining written payments policies that are updated frequently.

*A signature* is a recorded attestation that links a signer with information. The signature both authenticates the signer and associates a signer with one or more specific transactions. The financial industry commonly uses conventional pen-and-ink signatures on checks. In addition, a *digital signature* provides a similar service in the electronic space. A digital signature not only authenticates the user identity and data before processing the transaction, but it also provides cryptographic after-the-fact evidence of the transaction in a cryptographically secured log record. To be effective, digital signatures use sophisticated cryptographic technology to make them very resistant to forgery.

**Greater Accountability is the Order of the Day**

Federal mandates have done much in recent years to make information security a high priority for corporations and financial institutions. For example:

- The Federal Financial Institutions Examination Council (FFIEC), established in 1979, is a formal interagency body empowered to prescribe uniform principles, standards and report forms for the federal supervision and examination of financial institutions by the Board of Governors of the Federal Reserve System (Federal Reserve Board, or FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the Department of the Treasury’s Office of Thrift Supervision (OTS). A recent mandate in the United States requires multifactor authentication or layered security for Internet payments or display of confidential customer information.

- The Sarbanes-Oxley Act of 2002 requires that officers of publicly traded U.S. companies certify the accuracy of information contained in the public filings for which they are responsible, including a certification stating that the reporting officers are responsible for establishing, maintaining, and assessing the effectiveness of internal controls to ensure the veracity of the information reported. This certification requirement and the corresponding penalties for false certifications have amplified the importance of establishing administrative, technical and physical safeguards for information contained on public companies’ IT systems.

- Basel II, a set of international regulations designed to promote financial stability by encouraging banks to identify and manage risk more effectively, has imposed regulations requiring large financial institutions to measure their risks, including the security of their customers’ private information.

The rules and regulations created and enforced by these bodies have done much to drive the implementation of information security policies across all industries. But they are only the beginning. It
remains imperative for every enterprise to develop and enforce policies and processes that satisfy the unique demands of its particular company, industry or constituencies.

How JPMorgan Chase Addresses Information Security

As technology has successively enabled powerful new business capabilities, JPMorgan Chase has kept pace by proactively updating information security measures to include the latest proven technologies and protocols. JPMorgan Chase has an Information Technology Risk Management program that meets or exceeds the requirements of the OCC and the FFIEC, as well as the Gramm-Leach-Bliley Act and other applicable data privacy laws and regulations. The combined features of the JPMorgan Chase information security program help to provide reasonable assurance that appropriate procedures are in place to:

- Protect customer information, in any form
- Monitor systems, protect them against viruses and other threats, and enable them to recover quickly from incidents
- Assess whether JPMorgan Chase suppliers adhere to the firm’s security policies and standards
- Help employees understand their responsibilities to comply with IT Risk Management policies and standards

Secure digital signature with multifactor authentication

Portal Security Transaction Protocol (PSTP) is a patent-pending cryptographic digital signature technology developed by JPMorgan Chase. PSTP authenticates the credentials of a customer who seeks to transfer funds using an Internet browser. The customer then applies a PSTP digital signature with extremely high antiforgery security to his or her transactions.

The PSTP signature has three components: the authenticator, which contains the credentials that authenticate the user; the message integrity component, which secures data; and the key management component, which fuses the first two components together. Although it is not the only solution in the industry that cryptographically binds user credentials to data, PSTP is simpler and more portable than traditional certificate technologies. The secret behind JPMorgan Chase’s implementation of PSTP is that its authenticator leverages a stringent multifactor authentication process that utilizes the RSA SecurID® token—a solution that simultaneously simplifies and strengthens the online authentication process.

A legitimate user begins by entering both a personal identification number and the number being displayed in real time on the assigned RSA SecurID token. The token generates an authentication code every 60 seconds. Once the user enters the correct information, the server on the other end of the transmission verifies the number the token is supposed to be showing at that moment and checks it against the user’s entry. Then the server either allows or denies access.

Using advanced encryption technology to help achieve end-to-end transaction security, PSTP technology provides secure log records in the audit trail for both the originator of the transaction and the recipient. Digital signing binds users to the transactions they initiate, simplifying and securing tracking and auditing. This process also helps to prevent invasion into corporate databases by hackers and viruses.

Permissions technology

JPMorgan Chase augments its powerful authentication measures with stringent authorization protocols to help to ensure that users—whether employees or customers—have the ability to access many applications, but are able to use only the applications and information for which they have been granted authorization.
Check fraud measures
To help customers prevent fraud in check transactions, JPMorgan Chase offers positive pay and reverse positive pay, as well as powerful ACH debit blocks and filters. The bank also employs internal operational protocols—including controlled access to payment processing, daily account reconciliation, discrete disbursement and reconciliation duties—and frequently reviews and updates its policies.

Other tools include Payee Verification, an enhancement to positive pay that matches the payee line of presented checks to the issue file provided by customers. Discrepancies are reported as exceptions for a pay or return decision. Reverse positive pay provides a paid transmission file to subscribing customers each day, against which they match their issued checks and send instructions to the bank to either pay or return.

Customers can also establish a maximum dollar threshold that automatically returns checks unpaid if they exceed the designated dollar limit. Stale dating automatically returns checks to subscribing customers for a pay or return decision if the checks are presented after a predetermined honor date. In addition to check fraud services, imaging features such as bar-coding, seal-encoding, watermarks, micro printing, thermochromic ink, warning bands and chemical voids help reduce the risk of check counterfeiting.

Penetration testing methodologies
In addition to monitoring its own proprietary applications, JPMorgan Chase conducts ongoing penetration testing by third-party organizations to help ensure compliance with the company’s security standards.

Disaster recovery
The tragedies of September 11, 2001, and Hurricane Katrina in 2005 reinforced dramatically that having secure data on-site in a main data center isn’t enough. To minimize the risk of widespread data loss due to weather or other disasters, as well as to optimize network performance, the JPMorgan Chase Business Resiliency program strengthens business continuity and the safety and availability of its systems and information with redundant data centers located throughout the country.

Secure e-mail
While it is ultimately incumbent upon an e-mail recipient to be on the lookout for suspicious e-mail, JPMorgan Chase uses several methods to identify its outgoing e-mails as legitimate and secure. Company e-mails explicitly identify recipients by name. Additionally, if customers are directed to a Web link in a JPMorgan Chase e-mail notification, the URL is clearly spelled out with an unequivocal JPMorgan Chase identity in the Web address.

As part of its online customer education resources, JPMorgan Chase also provides explicit guidelines to help customers identify fraudulent e-mails and avoid victimization. For example, JPMorgan Chase will never request personal or security information via e-mail.

Robust infrastructure
JPMorgan Chase has an IT infrastructure designed with application and information security in mind. It includes:

- A multitiered IT architecture that provides multiple levels of firewalls between the Internet perimeter and the intranet, configured with ingress and egress filters and designed with multiple levels of defense, including two-factor authentication
- Internal partitioning with carefully enforced authorization policies
- Intrusion detection sensors that monitor anomalous activity with filters for various attack signatures, 24 hours a day, seven days a week
- Antivirus technology infrastructure that addresses malicious code at the gateway, server and client levels, using multiple technologies to mitigate the risks related to new viruses and worms
- Content controls at Web and e-mail gateways to help prevent the introduction or release of potentially malicious code, inappropriate communications or leakage of confidential information
- Cryptographic security standards and processes that control cryptographic keys, including the management of digital certificates and use of code signing capabilities as deemed appropriate
- Interconnections to support hardware and software cryptographic solutions
- Caching devices and proxies to protect the environment from inappropriate content and services

**Stringent internal security**
Within the secure JPMorgan Chase IT environment, data is classified and protected to prevent unauthorized access, with policies and standards clearly articulating the proper handling and protection of enterprise and customer information. In addition, JPMorgan Chase’s internal Infrastructure Operations Center provides continuous monitoring of system performance, data centers, operations centers and other key buildings and assets to ensure the security of information and customer transactions, as well as the integrity of the IT infrastructure.

On a daily basis, an enterprisewide Incident Response Team works to identify and address any vulnerabilities in accordance with JPMorgan Chase’s IT Risk Management standards, and manage any security issues that may arise. Internal audits and vulnerability assessments are conducted on a regular basis, plus regulatory oversight of IT applications and e-business infrastructure is conducted by both an internal Information Security team and independent third parties.

Augmenting these stringent controls is the previously mentioned JPMorgan Chase Business Resiliency program, which is regularly tested to help to verify that critical applications and systems will continue to function in the event of any natural, man-made or technology disaster.

**Transacting Business Will Always Involve Risk**
Effective information security requires more than implementing the right type of technology. It must also address the technology, processes and people within the enterprise. Since no enterprise remains static, information security needs to adjust and evolve as the company changes its processes. When a new process is introduced into the operational area, for example, it helps to assess how the new process will impact the existing information security system, and what types of employee training are needed to accommodate that change.

It's unrealistic to believe that any company can eradicate all possible misuse of its information. However, companies can go beyond a reactive, “bandage” type of approach to security threats and, instead, create a proactive defensive framework. This framework begins with:

- **Creating a risk assessment methodology**: A formal risk assessment process provides a sound foundation for defending against information security breaches. The idea is to determine how vulnerable a process or application is to an attack—including threat probability and the consequences of an actual attack on that process or application—and balance that against what would reasonably be needed to mitigate vulnerability based on the type of information contained within that process or application.

- **Identifying necessary security resources**: Once testing determines that an application or process is vulnerable to a hacker’s attack, decide the type of resources needed to mitigate that risk, based on the level of vulnerability that exists and the degree of confidentiality or sensitivity of the information. If the information is deemed less sensitive, applying the heaviest coat of security may be overkill.

- **Categorizing sensitivity levels**: Categorizing different types of data by degrees of sensitivity and establishing acceptable levels of information security for those different data categories will help fine-tune information security risk evaluations. Data with similar criticality should be protected in equal measure no matter where it happens to reside. Many companies find it useful to assign risk ratings to different data categories.

- **Establishing an update/educate schedule**: Companies that excel in information security update their antivirus software regularly, educate employees about the importance of avoiding unsolicited e-mail and protecting their passwords, and diligently enforce their information security policies.
• **Adhering to a regular maintenance schedule:** Once security measures are implemented, it’s important to maintain oversight. Companies should establish formal procedures and schedules for the maintenance, upgrading and monitoring of information systems.

• **Selecting suppliers and partners judiciously:** Every enterprise is vulnerable to the security weaknesses of other companies with which it does business. To ensure the safety of one’s own systems, it is always advisable to do business with companies that have a long and proven track record of diligence and success in the area of information security.

By following these guidelines, companies can significantly minimize their information security risk.

**To learn more**

JPMorgan Chase remains committed to providing the highest level of information security available for its clients. We invite you to find out more about how our firm protects the people we serve. For more information, visit http://www.jpmorganchase.com/ts.