System Security

Need of The Hour

Prasad Gupte

PGDBA (E-business)

CISA, CISM, ISO 27001 LA , ITIL-v2

Agenda

- 1. What is security
- 2. Why is IT Security necessary
- 3. Regulatory and Compliance requirements in India
- 4. How to achieve Systems Security (VA/PT, Appsec, Source code review etc.)
- 5. Risks like Phishing, Identity Theft, Industrial Espionage, Loss of customer / investor confidence, Financial and Legal penalties
- 6. New challenges like Cloud, BYOD

What is Security?

- Systems security is a ‘Business Issue’ not an IT problem
- Threats to Information Systems are threats to Business
- A *threat* is a danger which could affect the security (confidentiality, integrity, availability) of assets, leading to a potential loss or damage
- Security is the protection of information systems and services against disasters, mistakes and manipulation so that the *likelihood* and *impact* of security incidents is minimized
- The objective of system security is: *“to put measures in place which eliminate or reduce significant threats to an acceptable level”*

Information Systems Security is Comprised of:

- *Confidentiality:* Sensitive business objects (information & processes) are disclosed <u>only</u> to authorised persons

- *Integrity:* The business need to control modification to objects

- *Availability:* The need to have business objects available when needed

- *Legal Compliance*: Information/data that is collected, processed, used, passed on or destroyed must be handled in line with current legislation of the relevant countries

Why is Security Important?

- **If there is a weakness in your IT security system, wouldn't you prefer to find it before someone else does?**

- Most companies use electronic information extensively to support their daily business processes
- Data is stored on customers, products, contracts, financial results, accounting etc.
- If this electronic information were to become available to competitors or to become corrupted, false, stolen or disappear:
  - *What would happen?*
  - *What would the consequences be?*
  - *Could the business still function?*

Common Causes of Damage

- Human Error 52%
- Dishonest people 10%,
- Technical Sabotage 10%
- Fire 15%
- Water 10%
- Terrorism 3%
- *Who causes damage?*
  - Current employees 81%, Outsiders 13%, Former employees 6%
- *Types of computer crime:*
  - Money theft 44%, Damage of software 16%, Theft of information 16%, Alteration of data 12%, Theft of services 10%, Trespass 2%

How Much Security ?

- Systems with different requirements need to be secured in different ways

- A balance should be found between too much security (very restrictive use, high cost) and too little security (unrestricted use, danger, low "visible" cost)

- The value of information and processes should be known, the risks in the current environment analysed, so that an appropriate set of countermeasures can be implemented. A cornerstone of countermeasures is ***risk analysis*** and the ***security policy***

Security requirements are often specified in terms of:

- *Assurance:* Confidence that a System behaves as expected (i.e. according to it's specification)

- *Identification / Authentication:* During communication with each other, the two parties must identify each other, such that they know who they are communicating with

- *Accountability/Audit Trail:* The ability to know who did what, when, where. Users are responsible and accountable for their actions

- *Access Control:* Access to specified resources can be restricted to certain entities

Security requirements are often specified in terms of:

- *Object Reuse:* Objects used by one process may not be reused or manipulated by another process such that security may be violated

- *Accuracy:* Objects (information and processes) are accurate and complete

- *Secure data exchange:* Confidentiality, Integrity, Authentication, Non-Repudiation of origin and recipient

- *Reliability of service*: Data and vital services are available when needed

Business Impact and Risk Assessments

- In order to understand the security risks that an organisation faces, it is necessary to undertake a risk assessment
- A risk assessment will identify an enterprise's key information assets and perceived security threats, and assess them based on *probability* and *risk*
- This will ensure that appropriate mitigation strategies are put in place which focus resources on the *most* critical assets

- There are international standards which specify risk management approach and methodologies:
- ISO 27001 (formerly BS7799 Part 2)
- ISO 27002 (formerly ISO/IEC 17799 / BS7799 Part 1)
- ISO/IEC 31000 Risk Management
- ISO/IEC 25999 business continuity standard for IS Management Systems

Compliance and Regulatory Standards

- The regulatory and compliance climate is becoming more demanding and complex
- Therefore, there is a need for assessing organizational policies, procedures, and technical implementations against key local and international industry standards
- The following standards are important:
  - ISO 27001 (formerly BS7799 Part 2)
  - ISO 27002 (formerly ISO/IEC 17799 / BS7799 Part 1)
  - ISO/IEC 25999 business continuity standard for IS Management Systems
  - ISO/IEC 31000 Risk Management
  - COBIT 5.0: Control Objectives of Information and Related Technology
  - RBI Guidelines on - Internet Banking and Technology Risk Management
  - Indian IT Act 2000
  - Indian IT Act 2008 amendment
  - PCI:DSS Payment Card Industry (PCI) Data Security Standard (DSS)
  - Sarbanes-Oxley (SOX) Section 404: Management Assessment of Internal Controls

Penetration Testing & Vulnerability Assessments

- Penetration testing (ethical hacking)
  - Tests the security of IT systems, by identifying and exploiting weaknesses
  - From the perspective of its most likely threats, looking at business processes, information flows and the technology that supports operations
  - Determines the resilience of the environment to malicious attempts to penetrate IT systems

- Vulnerability assessments
  - Use testing tools (vulnerability scanners) to identify security vulnerabilities in a system or environment.
  - Highlight the technical threat, do not qualify the business threat
  - Does not assess common attack methods

- *The major distinction between a vulnerability assessment and a penetration test is that the vulnerability assessment does not actively exploit the identified problems to determine the full exposure or validate its existence which can lead to inaccuracies in the report (false positives)*

Importance of Penetration Testing

- **Penetration Testing (Pen Test) as Part of Corporate Governance**
  - Pen tests are a requirement for meeting regulations such as RBI Guidelines, IRDA, PCI DSS, SOX, and HIPAA. It is also defined in industry standards such as ISO 27001 as important security tests an organisation should regularly undertake
- **Key Pen Test Technology Focus Areas**
- Traditional Pen Test disciplines:
  - Network Pen Test (infrastructure Pen Test), e.g. router, switch, firewall, etc.
  - Server Pen Test, e.g. operating system, application, etc.
- Advanced Pen Test technology disciplines include, but are not limited to:
  - Application
  - Virtualization
  - Database
  - BlackBerry Enterprise Server
  - Wireless
  - PBX / PABX including VoIP

Application Security

- Assessing application security - both web (browser based), non-web (client/server, compiled binaries, command line, etc), including front-end and back-end systems, is extremely important for all Banking and Financial organizations, E-Business, Defense, Government, etc.

- History has proven that software defects, bugs and logic flaws are consistently the primary cause of commonly exploited application software vulnerabilities. These can lead to unauthorised access of networks, systems, and applications information

Web Application & Web Services Security

- According to research by Gartner, an estimated 70% of all security breaches are due to vulnerabilities within the web application layer (attacks exclusively using the HTTP/HTTPS protocol). Traditional security mechanisms such as firewalls and IDS provide little or no protection against attacks on your web applications

- Methodology and Approach
- A web application security review identifies vulnerabilities inherent in the code of a web application itself, regardless of
  - the technology in which it is implemented, or
  - the security of the web server or back end database

- Specifically, it analyses the critical components of
  - a web-based portal,
  - e-commerce application, or
  - web services platform

Web Application Security Assessment

- As part of a web application security assessment, analysis of the following key areas within applications should be done:
  - Architecture
  - Business Logic, Functional Specification & Implementation
  - Authentication
  - Access Control & Authorization
  - Cryptography
  - Session Management
  - Data Validation
  - Error Condition Handling & Exception Management
  - Data Confidentiality
  - Management Interface
  - Privacy Concerns

Approach to Web Application Testing & Web Services Security

- Should be based on Open Web Application Security Project (OWASP) guidelines and it should be done by competent and experienced professionals

- Some of the typical web application vulnerabilities including, but not limited to:

Hidden manipulation
Configuration subversion
Buffer overflow
Vendor option exploitation
Access to administration areas and internal modules
SQL injection
Backdoors and debug options
HTTP Attacks

Improper management of permissions
XML/SOAP vulnerabilities
Parameter tampering
Cookie poisoning
Cross Site Scripting (XSS)
Stealth commanding
Forceful browsing
Directory traversals
Session hi-jacking
Denial of service
Information disclosure

Social Engineering

- Social engineering has emerged as one of the most successful attack vectors in recent times
- A social engineering attack is typically carried out by an external assailant who deliberately manipulates an employee's good intention (i.e. their willingness to assist) or their general curiosity, such as enticing them to click on a link in an email to a malicious website
- Common tactics used by social engineers include:
  - Tailgating - The social engineer closely follows employees into secure areas before the door has closed
  - Pretexting - A social engineer convinces an employee, in person or by phone or email, to hand over confidential information by impersonating someone else
  - Phishing - Sending an email which is disguised to appear as though it comes from a legitimate source and encourages the target to activate the attached malicious file or click on a link that directs the victim to a website hosting malicious code or requesting personal details
  - Baiting - This is where a social engineer leaves infected USB keys or other media in common areas such as lunch rooms, parking lots or foyers for employees to pick up and insert in their computers (Stuxnet – Bushehr nuclear facility incident)
- Organization must build the ability to defend itself against this type of attack method

A Source Code Review

- A source code review is an offline analysis of software code in a programming project with the intent of discovering common security design and coding flaws

- Source code reviews can be manual or automated. Also, audits for all major programming languages can be done

Host Security Assessment

- A host security assessment is performed from the view point of a host or devices console logged in with privileged access. It can provide additional insight into the servers' security configuration that cannot be seen from the network and allows for the identification of additional exposures and configuration weaknesses that may make a host more susceptible to compromise, or make a successful compromise more effective

- Specifically, it ensures the host's operating system and applications have been appropriately "hardened" to give you the best protection against existing risks as well as new and emerging threats

- The assessment should conducted with reference to industry leading methodologies, such as the SANS Network Security Audit Methodology and the Centre for Internet Security benchmarks

Host Security Assessment Contd..

- The assessment method is based on a configuration review, a desktop review of available information and documentation, complemented by interviews with the system administrator.
- Some of the technologies reviewed include, but are not limited to:
  - Routers
  - Switches
  - Firewalls
  - Load balancers
  - Intrusion detection systems
  - Operating systems
  - Web proxies
  - Web servers
  - Application servers
  - Mail servers
  - Database servers
  - Virtualisation implementations
  - Wireless
  - BlackBerry
  - PBX - including VoIP

Database Security

- Database servers have become the foundation of today's systems. Demand for online and real time access to information has brought database systems closer to the perimeter where they are increasingly being used to hold more and more sensitive information. E.g. financial data, personal data, credit card numbers. This makes them more vulnerable than they have ever been before – and hackers are realizing this and actively targeting organizations "crown jewels"

- Databases are extremely complex systems and difficult to correctly configure and secure. As a result serious security vulnerabilities and mis-configurations frequently go unchecked or completely undetected

- To understand organization's security exposure, it is vital to conduct a thorough assessment of database servers before deployment, and then on a defined regular schedule

- Different database platforms and technologies are:-. SQL, Oracle, Sybase, MySQL, DB2

Wireless Security

- Wireless networks, specifically 802.11, have become popular due to their lower cost, ease of deployment, and flexibility. However, this new technology brings with it a set of unique security risks which many organizations fail to consider

- Wireless networks use radio signals to carry network traffic, and are vulnerable to eavesdropping by anyone with a PC and wireless network card. If they are not properly protected, the emitted signals can be intercepted kilometers away

- Most wireless access points are designed with ease of use in mind, rather than security. Although security features are usually available, these are commonly disabled by default. Integrating wireless into your existing network requires expertise to ensure you are not exposing your organisation to new security threats

- Even if company's IT department hasn't chosen to deploy wireless technology, can you be sure none of your employees have? Wireless that has not been properly secured can render existing wired security measures such as firewalls ineffective

Wireless Security Contd..

- The only way to ensure that your organisation is not exposed to wireless security threats is to perform routine audits covering all the major spectrums:
  - Wireless Security Services
  - Test for the presence of wireless access points - As mandated by PCI Requirement 11.1
  - Wireless Site Survey
  - Secure Wireless Design and Implementation
  - Wireless Security Assessment, Review, Audit
  - Wireless Penetration Testing

Telecom Security

- Telephone network hacking (phreaking) and fraud is becoming a serious problem globally. Each and every day an organisation suffers a major loss from hackers (average cost $78,000). Anyone with a telephone or voicemail system is at risk.

- An attacker who has compromised your system can:
  - Make toll calls at your expense
  - Listen to your voicemail
  - Maliciously reprogram your system
  - On-sell the use of your system to others
  - Disable your organization’s voice communications

Telecom Security Contd..

- Security measures are required to be taken to pinpoint vulnerabilities and mis-configurations in system (both traditional PBX/PABX and VoIP based) by performing comprehensive testing and analysis (telecom audit) of telephone system and voicemail

- Use similar tools and techniques that a phreaker (phone hacker) would. If we can get in so can competitors, a disgruntled employee or a phreaker. In addition, complement this with an assessment of architecture and a review of security configuration in order to identify ways to improve robustness to attack

SCADA Security

- What is SCADA?
- SCADA is an acronym that stands for Supervisory Control and Data Acquisition. SCADA refers to a system that collects data from various sensors at a factory, plant or in other remote locations and then sends this data to a central computer which then manages and controls the data.

- SCADA is a term that is used broadly to portray control and management solutions in a wide range of industries. Some of the industries where SCADA is used are Water Management Systems, Electric Power, Traffic Signals, Mass Transit Systems, Environmental Control Systems, and Manufacturing Systems.

- SCADA based systems usually exert significant control over core infrastructure and the disruption of these services could have catastrophic events. These systems are usually diverse, cover various physical locations and are obscure in implementation and management. (Stuxnet - Iran nuclear facilities at Bushehr, Natanz hacked)

Need to Audit SCADA Based Systems?

- In recent times the security of SCADA based systems has been called into question due to highly publicized successful intrusions that has, in some extreme cases, resulted in an external party obtaining administrative access to core systems
- It is predicted these systems will increasingly become a greater target for cyber attacks, denial of service and physical disruption. In order to ensure that SCADA based systems are secured from external threats, self assessment and external independent audits should be conducted regularly
- Stuxnet - Iran nuclear facilities at Bushehr, Natanz hacked

Virtualization Security

- Virtualisation software allows you to run multiple operating systems on a single machine at the same time
- Virtualization technology is gaining popularity due to the benefits it offers in terms of reduced costs and increased operational efficiency and flexibility
- However, this technology introduces a virtualisation layer that itself becomes a potential avenue of attack for the virtual services being hosted
- Because a single host system can house multiple virtual machines, the security of that host becomes critical in maintaining the confidentiality, integrity and availability of your systems and data
- This new technology is often poorly understood, and rarely implemented correctly in enterprise environments without jeopardizing the organizations security posture

Virtualization Security Considerations

- There are a number of security considerations which differ from the physical world, including but not limited to:
  - network architecture
  - zones of trust, network segmentation, and access control
  - virtual switches and networking
  - virtual appliances
  - mobile servers
  - patch application and management
  - intrusion detection and prevention
  - definition of roles and responsibilities
  - storage

Mobility Security

- Modern mobile devices and smart phones:
  - Introduced new risks to a corporate network environment
  - Ever increasing complexity and capabilities
  - Security of these devices becomes critical in maintaining the confidentiality, integrity and availability of your systems and data

- Mobility Platforms:
  - iPhone
  - BlackBerry
  - Android devices
  - Symbian devices

- Mobile technologies are advancing at very high pace, where enterprises are not able to adapt their procedures and processes to deal with new risks and challenges. This may jeopardize the organizations security posture

Mobility Security Considerations

- There are a number of security considerations which are often not considered for mobile devices and smart phones, including but not limited to:
  - Mobile device management and monitoring
  - Device jailbreaking
  - Zones of trust, network segmentation and access control
  - Patch application and management

Perimeter Security & Content Security

- **Perimeter Security**
- Firewalls are critical component in enterprise security environments
- Even the most expensive firewalls can be rendered useless when not properly integrated, and the policy they enforce is not well thought out and effectively implemented
- Understand business requirements, processes and functions, translate these into an effective design and policy which can be enforced within the context of the current threat environment

- **Content Security**
- Is concerned with mitigating the security threats and problems associated with the flow of digital content in to, out of, and within an organisation
- Increased sophistication of threats and blended attacks requires a holistic approach to content security that spans a variety of technologies and provides for a co-ordinated defense
- These technologies encompass the protection of email, web traffic, instant messaging and peer-to-peer (P2P) networking

Intrusion Detection & Prevention

- Intrusion Prevention Software (IPS) is designed to detect and protect against inappropriate, incorrect, or anomalous activity that is aimed at disrupting the confidentiality, integrity, or availability of a protected network and its computer systems

- An IPS collects information on a network, analyses the information on the basis of a preconfigured rule set, and then responds to the analysis in real time to provide protection

- Intrusion Detection Software (IDS) has evolved from providing simple real time alerting to provide comprehensive network protection – i.e. IPS

- Effectively integrating this technology into enterprise environments requires competence and experience

Remote Access & Strong Authentication

- **Remote Access**
- With the increase in globalization and tele-commuting, effective remote access solutions are fast becoming a necessity in conducting business
- Enterprises implement secure remote access solutions utilizing dial-up, client Virtual Private Networks (VPNs), clientless VPNs (SSL VPN) and site to site VPNs

- **Strong Authentication**
- It is important to ensure that you can reliably authenticate who is accessing your data
- Simple password protection is no longer sufficient
- A comprehensive range of two-factor, PKI or certificate based solutions that are specifically tailored to meet evolving security envionments

Server and Application Hardening

- It is critical to define and implement workstation and server operating system and application baseline standards (secure configuration guides) for all types of organizations
- Various hardening guides (standards) for Windows, UNIX and Linux, are available in the marketplace
- Standards based on industry leading practices (such as SANS, NSA, NIST and CIS) and designed to meet a high level of security, whilst maintaining any administration, maintenance and backup requirements are important.
- It is not enough to secure current environment, but also to put policies, procedures and guidelines in place to ensure that new problems are not introduced

Patch Management

- Failure to install the latest security patches is a **leading cause** of security breaches and worm infections
- 'Patches' are commonly released by software vendors to rectify critical system stability and security related bugs which are found to exist in a product sometime after its initial release
- Many victims of recent internet worms such as Code Red, Nimda, Slammer, Blaster and Sasser, could have avoided intrusion by simply having kept their system patching up to date
- Patch management is **as much about process** as it is about technology, and needs to operate in conjunction with internal change management processes
- It is important to deploy patches **regularly and effectively** without adversely impacting the operating environment
- Installing patches is an ongoing challenge, but is a necessary part of **diligent system administration**
- It can be extremely time-consuming for a system administrator to research new patches and analyse which systems might be affected
- In addition, patch dependencies and patch supercedence can further complicate the process and may lead to additional exposures

Disk Encryption

- Theft and loss of portable computers has increased dramatically in recent years
- Portable PC's can hold tremendously sensitive data relating to company secrets or personal privacy
- The comparative mobility of portable PC's makes data on them vulnerable in a way that data on servers and desktops is not
- The size of portables makes them easy to steal, as employees commute and travel with them presents ample opportunities of both loss and theft
- While loss and theft of computer hardware can result in substantial monetary costs**, it is often more important to ensure that the data on stolen portable computers cannot be accessed than recovering the hardware**
- This has been highlighted by a number of recent high profile incidents where company records were stolen as a result of laptop theft
  - *For example, in August 2003, Well Fargo & Company lost more than 200,000 personal records when a thief stole one laptop belonging to the bank's consultant*
- Implementing enterprise disk encryption solutions will address this issue to considerable level. The enterprise disk encryption solutions can be centrally managed and maintained and will be invaluable in preventing these types of exposures

Endpoint Integrity

- In today's highly connected world there is an expectation that access to systems and data will be available from anywhere anytime
- It is this demand for real time access from any location that dramatically increases our risk profile
- Today's employees are using a variety of devices such as laptops, smartphones/TABs, and removable media to access corporate data and resources
- The corporate network is expanding beyond the previously defined perimeter
- A solution must be found to evaluate the integrity of an endpoint, including the appropriateness of its security controls, before access is granted
- In a role-based access environment the evaluation criteria may be complex and the enforcement controls even more so, do not leave the integrity of your enterprise to chance

Data Loss Prevention

- Even a simple network can have more entry and exit points than one might imagine. This along with today's voracious appetite for information on demand presents multiple channels to funnel corporate information into and out of enterprise systems
- Unfortunately many of these channels are either not monitored, or perhaps not even known, and they present an opportunity for sensitive information to be lost and leaked
- Email is the most prolific avenue for data loss.
- USB keys and other portable media such as external hard drives, CD/DVD etc all provide high density, low form factor options to extract information from corporate systems
- Laptops themselves are designed to be portable devices and are frequently lost or stolen with inordinate amounts of sensitive data on them
- A number of technologies exist which can be deployed to address the various loss vectors (e.g. encrypted laptop hard disks, encrypted USB keys, email gateway monitoring). When these are combined with appropriate governance they can provide an effective solution to data leakage across the enterprise

Data Destruction

- Also known as **data sanitisation** or **data wiping**, is the ***permanent and irreversible*** removal or elimination of data from modern media storage devices
- It is achieved by a variety of secure methods and ensures that sensitive information about your organisation, employees and clients is not vulnerable to unauthorised access and misuse
- Secure data destruction should be an essential part of any enterprise or corporate IT strategy
- Most importantly data theft is an ever present threat. Critical data that could be lost includes:
  - customer information
  - intellectual property
  - financial plans
  - marketing strategies
  - research and development

Risks & Secure Data Destruction

- Modern software typically does not erase a file when deleted, it merely archives the item and removes the visible link. Data therefore remains on the storage medium, and is vulnerable to recovery by forensic software

- Other deletion methods such as reformatting, repartitioning or overwriting of hard drives are also susceptible to analysis by dedicated software, and are not a secure form of data destruction

- Poor information security and the resulting loss of sensitive data raise the risk of a number of potentially damaging scenarios

- **Secure Data Destruction:** Following are secure methods of data destruction:
  - Clearing - a method of overwriting on media with non-sensitive data
  - Degaussing - erasure of data on magnetic storage devices such as floppy disks and tapes
  - Purging - permanent removal of sensitive data from a variety of media
  - Physical destruction - CD/DVDs

Various Threats to Data

- ***Phishing*** involves the capture and criminal abuse of personal information, typically via fraudulent e-mail messages or fake web site designed to steal your identity
- ***Phishers*** impersonate a reputable individual, company or organisation such as your bank, in attempt to secure your user credentials
- ***Spear phishing*** is a refined form of phishing typically targeting an entire company, institution or organisation with the intention of gaining access to its entire system
- ***Identity theft*** refers to the procurement of personal or sensitive information that is then used by a criminal to impersonate a person or business, typically for financial gain
- ***Industrial espionage*** is an attempt to gain access to information about a company's plans, products or clients for commercial gain
- ***Loss of consumer/staff/investor confidence*** often results if sensitive consumer data is breached or compromised. This can irrevocably affect a company or brands reputation and can result in a loss of earnings
- ***Financial and/or legal penalties*** can result if **due care** is not taken of **sensitive personal and corporate** data. Substantial regulatory fines are becoming the norm

Mobile Banking Security

- How secure is mobile banking?
- Could a thief sniff out your bank account information digitally?
- Is it safe to make financial transactions using an app or text messaging, or by visiting a mobile Web site?

- Mobile banking is somewhat secure because,

- There are many variations of banking apps and methods;

- A thief cannot predict which a potential victim might use;

- There is no one standardized method otherwise, the story might be different.

- Even so, there are certain rules you should follow to make sure your banking information remains safe

Tips for Secured Mobile Banking

- **Don't Follow Links**
- You should never follow a banking link sent to you in a text message or e-mail
- It's always a good idea to navigate to a Web site directly
- Enter your bank's Web address into your phone and bookmark it
- You should never send your account information or password via text message or e-mail

- **Avoid Banking While on Public Networks**
- Before you log into your account, make sure you're not connected to the public network
- Public connections aren't very secure
- If you're using a smart phone or other cellular device, disabling the Wi-Fi and switching to a cellular network is a good solution
- Most smartphones connect to the Internet using either a wireless Internet connection or a mobile provider network, which is the most secure option.
- Your best bet is to connect using your smart phone's 3G or 4G network or your password-protected home network, which are much more difficult for the bad guys to intercept data from
- Never store your passwords on mobile device, it is secure entering your username and password each time

Tips for Secured Mobile Banking Contd..

- **Use Official Bank Apps When Possible**
- Many banks now offer official applications in smart phone and tablet app stores. Generally, these apps tend to be more secure than sending information by SMS message or e-mail
- Ensure that your bank sanctions the app before you download and install it. Most banks will include a section on their Web sites to let you know about the official app
- Never send text messages to your bank about your account because text transmissions don't travel over a secure network
- If your bank, credit union or credit card sends you a text even if it doesn't contain sensitive information, don't store it in your phone
- **Get the Updates**
- If you aren't performing these updates, your banking information may become vulnerable to hackers who prey on software weaknesses
- Just make sure you're downloading your bank's official app by getting it straight from your bank's Web site instead of an app store
- Always check for application updates on a regular basis and then download those for use
- For added security, use your banking app to sign up for account alerts

Tips for Secured Mobile Banking Contd..

- **Keep Track of Your Mobile Device**
- Mobile devices contain everything from passwords to contact lists to our calendar appointments, information like that can be dangerous if your mobile device falls into the wrong hands
- If your device has a digital locking mechanism you should use it
- Some devices require you to trace a pattern or insert a PIN, that layer of security might be enough to keep a thief from accessing your bank account before you can report your phone as missing
- You should password-protect your smart phone
- General security like creating a strong password, should be followed when banking with your smart phone, too
- Do not accept to remember your password, refuse the convenience. It's better to manually enter the password each time than to risk storing it

Tips for Secured Mobile Banking Contd..

- **Be Prepared to Clear Your Data**
- The best thing: Data wipe apps that can be activated remotely
- A remote wipe app will reset your smart phone to its original factory settings, erasing your personal data like your contacts, emails or banking information. There are a variety of data wipe apps, including the Mobile Defense app for Android smartphones. The data wipe process is a little more complex for iPhone users; it requires a MobileMe account, a Find My iPhone app and the activation of push notifications

- If you have an iPhone, install the Find My iPhone app, which can locate lost or stolen devices via GPS and clean out your personal information. If you have an Android-based smart phone, apps like WaveSecure offer similar services

- Don't be scared off from using your mobile device to access your bank accounts. Just be sure to practice good, safe behaviors and keep track of your gadgets. With a little common sense and attention, mobile banking can be both convenient and secure

BYOD An Enterprise-Wide Consideration

- A BYOD policy should accommodate its employees' lifestyles and work habits while protecting employees and the organization from risk
- The organization needs to decide which platforms will be supported and how. This includes determining whether to support BlackBerry, iOS, Android, Windows, or Symbian operating systems (or some combination of those)
- At minimum, the organization must answer the following questions:
  - What devices and mobile operating systems can we support?
  - What are our security requirements at each level: devices, applications, and data access?
  - What risks are we introducing by letting employees access corporate data through their personal devices? What level of tolerance do we have for those risks?
  - How can we manage our mobile deployment in a BYOD world without risking sensitive data or intruding on employee's rights to privacy on devices they own?
  - Will we provide intranet access to BYOD users?
  - What types of users will be provided with BYOD devices? Will we provide them to everyone, or a select group that has a greater need for mobility?
  - What levels of access to applications and services will be afforded to each group of users?

BYOD – Managing Risks

- **Managing Risk of Corporate Data Loss**
- Fundamentally, an IT department must develop practices that protect corporate data while maintaining employee productivity. This involves the participation and cooperation of other departments, including human resources, purchasing, legal, financial, and the lines of business that own the data. All policies about data protection need to be incorporated into the BYOD policy
- **Questions to Consider**
  - What are the risks for loss of corporate data or intellectual property?
  - How is corporate content on employee devices managed without interfering with personal use?
  - Must users sign an acceptable use policy before connecting personal devices to the corporate network?
  - Is it legally acceptable to wipe corporate or personal data if the policy is violated and data is at risk of compromise?
  - How much data, such as GPS data, should we collect about users?
  - How should we handle lost or stolen devices?
  - Will our organization enforce the use of a “whole device” password?
  - Should and can we prevent jailbroken or rooted devices from accessing corporate data and apps?
  - What is our policy regarding use of devices by users other than the corporate end user?
  - What should happen if a user violates policy?
  - Should different violations be treated differently? (e.g., eligibility vs. security vs. acceptable use)?

Thank You