“What Hackers see beyond the Security Audit”

Niel Pandya, Senior Manager
Database Security ASEAN & SAGE
Agenda

• Hackers and Hacking
• The IT Security Audit
• Addressing the gap
• Adopting a sustainable model
• New Vectors
Do you SEE what the Hacker Sees?

Are you aware of your security posture?
Risks Are Increasing

- Cybercrime
- Malware
- Identity Theft
- Lost Laptops
- Targeted Financial Gain
- Personal information Sharing
- Slowing of security investment
- Dissipation of security message
- Competitive pressures
Why Cyber Attacks?

- The principal motives behind using the Internet for digital attacks include:
  - Creating political tension
  - Registering protest and digital warfare
  - Carrying out espionage, surveillance and reconnaissance
  - Causing destruction of competitive advantage or share price
  - Outlet for disgruntled or misdirected workforce issues
  - Symbolizing anti-globalization and anti-capitalism protest
  - Hacktivism: environmental and animal rights activism
  - Boredom: intellectual challenge and recreational hacking
  - Most Popular: financial gain
  - Most Critical: LOSS of HUMAN LIFE
Think about it

• Attackers can potentially:
  🔴 Shut off the electricity of a city
  🔴 Shut down the phone lines in a given neighborhood
  🔴 Cause a dam to release the water it is holding
  🔴 Cause two trains to crash into each other
  🔴 Many government experts assume that militant operatives will actually launch a cyber-attack in conjunction with a more conventional attack.
  🔴 For instance, terrorists could blow up a building and then disable the phone system in the surrounding area in order to prevent law enforcement, medical, and emergency officials from responding to the attack.
Why Terrorists use the Internet

- **Anonymity** - The Internet makes it easier for them to communicate covertly, preach to the public, and solicit funds.

- **Location Independence** - They can use it to plan and coordinate their attacks. The launch pad is no longer a runway, but a computer – the attacker, no longer a combat pilot, but a computer hacker bent on destruction.

- **Lesser tangible armory required** as well as lesser skill levels; as tools are available on the Internet. **Example:** John, a citizen, cannot go out and buy an F1-17 or Tornado fighter plane or an attack submarine. But with a relatively simple computer capability, individuals can do things via the cyberspace environment that can impact on the national security interests of actual nation states.

- **Ease of availing and transferring funds**

- **Extensive Reach of the medium**
Payment Card Data is Valuable

Menu

1 Quick Bites
Includes card number, expiration date, cardholder name and address, and the CVV2 security code.

US$1 - 9

2. Set Lunch (“full-info”)
Includes “cvv2” and enhanced with other data about the cardholder such as date of birth, mother’s maiden name, Social Security Number, place of birth, and other information for authenticating fraudulent transactions.

US$10 - 14

3. Chef’s Special (“dump”)
Includes credit card track data (electronic data from the magnetic strip on the back of a credit card).

starting from US$15
Normal instances and why you should be concerned! - 1

Does this sound familiar?
• “We have a good firewall, an anti-virus and know the people we work with.”
  • A good firewall can be mis-configured and turn out to be the best thing a hacker can use against you.
  • The anti-virus may not be updated and your system can be compromised.
  • The mail from your friend can turn your machine into a zombie for further attacks.
  • You could be held responsible for the attack by the law enforcement agencies!
Normal instances and why you should be concerned! - 2

Does this sound familiar?

• “We don’t transact on the Internet, so why would anybody hack our systems over the Internet?”
  
  • Your web server can be used as a “warez” house, even though you don’t transact? You could be hosting illegal files of questionable moral content.

  • A poll of more than 150 CIOs by IDG’s CIO Magazine found that two-thirds felt that information about a hacker attack would adversely affect their company’s valuation.
Normal instances and why you should be concerned! - 3

Does this sound familiar?

• “Our employees are so well connected that we work in real-time.”

  - Ever heard of spoofing? Information **can be stolen in real-time and sold** even before you can blink and click?

  - How sure can you be that the access point you have logged onto is not a **rogue access point**? - **FAKE ACCESS TO STEAL USER NAME/PASSWORDS**.

  - Are you really sure that **you** have not let a hacker take advantage of your **lack of awareness** and compromised your network?
Normal instances and why you should be concerned! - 4

**Does this sound familiar?**

- “I just browse and check my mail... I don’t see why or how I can be hacked.”
  - You can be hacked while **simply browsing** – you don’t have to click or open anything!
  - A poll of more than 150 CIOs by IDG's CIO Magazine found that **64 percent** of senior technology executives are worried about hackers stealing their e-mail and personal identity.
  - Identity theft can even drive **you bankrupt**!
Agenda

• Hackers and Hacking
• The IT Security Audit
• Addressing the gap
• Adopting a sustainable model
• New Vectors
What is Security Auditing?

- **Security Auditing IS**
  - Documenting security and other system events
  - ✓ Who changed a particular user profile?
  - ✓ Who deleted a specific logical file?
  - ✓ Who tried to access the Credit Card file?
  - ✓ Who changed a system value?
  - ✓ Who deleted a spooled file?

- **Security Auditing is NOT**
  - Journaling record changes
  - Capturing before and after images of file changes
  - Auditing payroll or financial records
Let’s Agree On This ....

• Auditors and Security Officers exist to ensure the business has:
  – Documented policies
  – Documented procedures/processes
  – Documented evidence of implementation these controls
  – Evidence of ongoing operations
  – Periodically tested the controls
What Do Security Officers LIKE about Auditors?

- Internal Audit areas usually have organizational clout
- Controls-oriented
- Can identify previously unknown issues
- Provide ammunition/urgency for fixing issues quickly
- Provide knowledge of best practices and standards
- Internal Auditors find issues prior to external audits
Reasons to use Auditing and Logging

- Laws and industry-regulations require auditing
- Internal or external auditors require it
- Your corporate security policies demand it
- You want to know what privileged users do on your system (i.e. command auditing)
- Keep track of object usage (i.e. how frequently an object has been accessed)
- Log actions, tasks, and access attempts of external partners and consultants
- Logging is important for tracking sensitive transactions and operations
- Job accounting
Why do a Security Audit?

• Information is power
• Expectations
• Measure policy compliance
• Assessing risk & security level
• Assessing potential damage
• Change management
• Security incident response
When to audit?

- Emergency!
- Before prime time
- Scheduled/maintenance
The Golden Rule of Auditing

• Verify ALL tools used for the audit are untampered with.
• If the results of the auditing tools cannot be trusted, the audit is useless
Agenda

• Hackers and Hacking
• The IT Security Audit
• Addressing the gap
• Adopting a sustainable model
• New Vectors
So what's wrong with IT Audit’s
Databases hold the crown jewels for organizations but often don’t get the strong focus they need when it comes to data security planning. Forrester estimates that although 70% of enterprises have an information security plan, only 20% of enterprises have a database security plan.
Two Thirds of Sensitive and Regulated Data Resides in Databases...

...and growing exponentially...

BUT IS IT SECURE?

Source: IDC, 2008
The need for Data

*We can no longer wait......*

a year ago – how many applications did you have, how many people, how many devices
Over 900M Breached Records Resulted from Compromised Database Servers

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>% Breaches</th>
<th>% Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Server</td>
<td>Servers &amp; Applications</td>
<td>25%</td>
<td>92%</td>
</tr>
<tr>
<td>Desktop Computer</td>
<td>End-User Devices</td>
<td>21%</td>
<td>1%</td>
</tr>
</tbody>
</table>

- Payment card: OffLine/Data 18% <1%
- POS server (store-centered): Servers & Applications 11% <1%
- Laptop computer: End-User Devices 7% <1%
- Documents: OffLine/Data 7% <1%
- UPS terminal: End-User Devices 4% <1%
- File server: Servers & Applications 4% <1%
- Automated Teller Machine (ATM): End-User Devices 4% <1%
- FTP server: Servers & Applications 2% <1%
- Mail server: Servers & Applications 2% <1%
Only 28% of companies uniformly encrypt personally identifiable information in all databases.

Only 23% encrypt database traffic.

Only 15% uniformly encrypt database backups and exports.

Independent Oracle User Group Security Survey 2010
The real value of audit solutions...

16 September 2011 Last updated at 14:03 ET

UBS trader Kweku Adoboli charged with fraud

Kweku Adoboli, the UBS trader alleged to have lost UBS $2bn (£1.3bn) in unauthorised trading, has appeared in court in London charged with fraud and false accounting.

He has been remanded in custody until a committal hearing on 22 September.

According to the charges, the fraud took place between January and September this year.

Mr Adoboli appeared before magistrates on Friday
Customer Pains

• *Heterogeneous* Database versions and brands
• 10’s to 100’s of databases all with auditing switched on but *no time* to check logs
• Incident happens long before it is detected
• Audit logs sit on servers where they can be tampered with – *not secure*
• Audit reports cost 100’s *per* report to develop
• Managing the audit from source to report is complex with many processes like collecting audit data, cleaning up audit logs, collating information and finally presenting this information in a report.
Audit Information should be ....

• 1) Complete
• 2) Current
• 3) Correct
• 4) SECURE

“Information systems should deliver good information”

....what about Audit Information?
Gartner says ....

By 2015, 10% of your online “friends” will be nonhuman.
Agenda

• Hackers and Hacking
• The IT Security Audit
• Addressing the gap
• Adopting a sustainable model
• New Vectors
Leading Organizations *Adhere To* This Model

- **Assess Risk & Determine Needs**
- **Implement Policies & Controls**
- **Central Management**
- **Monitor & Evaluate**
- **Promote Awareness**

Source: “Learning from Leading Organizations”
SGAO/AIMD-98-68 Information Security Management
Leading Organizations *Adhere To* This Model

- Assess Risk & Determine Needs
- Promote Awareness
- Implement Policies & Controls
- Monitor & Evaluate

Source: “Learning from Leading Organizations” SGAO/AIMD-98-68 Information Security Management
Information Security Strategy Must Align With Business Objectives

• Top-down process
• Linkages to business process and strategy
• Information in oral, paper, and electronic forms
• Transcends physical boundaries
• Establish acceptable practices, policies, and procedures
An Information Security Program With Governance Provides Increased Assurance

• Risk management
• Resource management of critical skills and infrastructure
• Performance measurement
• Providing value-add in delivery of services and products
• Specific Organizational accountability for security
Can Organizations Survive Without ...?

People
Computers
Buildings
Equipment
Few Organizations Can Survive Without

- Customer Information
- Knowledge of processes
- Accounting and financial reporting information
Fear Uncertainty Doubt Gets Investment $$$

EVENT + \text{REACTION/CONFUSION} = \text{INVESTMENT}
Security Needs Involvement From The Board of Directors/Executive Management

- Strategic Oversight
- Review alignment with organization strategy
- Determine Risk profile for organization
- Endorse security program
- Require regular reporting on effectiveness
- Review investment return
- Potential new technologies to add value, reduce costs
Multiple Groups Must Understand Security At The

*Appropriate* Level

- Competitive Disadvantage
- Fraud
- Loss due to disclosure, destruction of information
- Reputation/Public Confidence
- Bad decisions
- Business disruption
- Legal Liability
- Safety risks
- Loss of productivity
- Low Morale
- Corporate Espionage, loss of contracts
Focus Different, Goals Ultimately The Same

Management’s Objective

• Increase shareholder value (stock price)
• Increase revenue
• Reduce administrative costs
• Increase market share
• Increase worker productivity
• Provide innovative products
• Provide quality products and customer service
• Attract and retain talented workforce
• Accept reasonable business risk

Security Officer’s Objective

• Protect information from loss, destruction, unavailability
• Reduce risk of threats to acceptable level
• Implement effective controls
• Provide efficient service
• Enable secure development of new products
• Provide assurance through continuous control practices
Ensure Communication Plan Delivers Targeted Security Message

Manager Meetings → Tactical Plans
                      New Policies
                      Scheduled Activities

Strategic Initiatives → IT/Business Steering Committees
                      Policy Approval

Board of Director Meetings → Security Posture
                          Competitor Comparison

Interim Updates → Management Newsletters
               Issue Reinforcement

One-On-One Sessions → Departmental Issues
                     Testing Reality
Security Audits Necessary To Ensure Controls Are Functioning

Assess Risk & Determine Needs

Central Management

Monitor & Evaluate

Implement Policies & Controls

Promote Awareness

Source: “Learning from Leading Organizations”
SGAO/AIMD-98-68 Information Security Management
Agenda

• Hackers and Hacking
• The IT Security Audit
• Addressing the gap
• Adopting a sustainable model
• New Vectors
Introducing new vectors....

1) Cloud Computing
2) Mobile Computing
3) Social Networking
4) Consumerization of it
More People Worldwide Will Use Mobile Phones Rather Than PCs To Connect to the Internet

In Q4 2010, smartphones outsold PCs for the first time.
Social Networking

A new corporate experience in Engaging, Informing, Driving and Extending

Engage - Enterprise collaboration through real-time conversations.
Inform - Updates streamed from across your business.
Drive - Purposeful social networking without the noise.
Extend - Integrates into your business.
Consumerization of IT

Consumerization of IT: 95% of Information Workers Use Self-Purchased Technology for Work

Devices purchased by employee and used in work

- Employee purchased and used for business: 95%
- Not used for business: 5%

n = 2620
Consumerization of IT

So many operating systems - Apple, Android
More users turning up with own devices
- choice do we embrace that trend - take
advantage of the economics of this and also
provide
users with the tools they want - getting the
balance between protecting the enterprise and
user satisfaction
1) Celebrities
2) Royal Family
3) Victims of 7/7 London Bombings
4) Politicians

Who do you hold responsible if your phone conversation is hacked....
How we need to think about Security
Rethink Enterprise Software

Built At The Factory

Why can’t the software business work like every other technology industry in the world?

Design security into these new innovations
So What Needs To Change?

- Vertical Integration Across the Stack
- Modern, Open Standards
- Complete, Industry Solutions with compliance built in
- Security - Centric Architectures
- Economies of Scale
- Moving from reactive to proactive
- Security Intelligence
- Risk is systematically identified and the proper controls are put in place
- people - process – technology – incorporated with Business strategy and processes
So What Needs To Change?

- Unified communications and collaboration (uc & c) - team sharing, chat, document sharing
- Universal Identity
- Better /Controlled Information sharing
- Risk Management to include intellectual Property! (IT folks don’t really understand IP)
- end to end security starts with assessment of risk tolerance
- followed by compliance requirements
- operational requirements
- organisational capabilities and resources
- Protect Data at Source
MOST IMPORTANTLY!

• Build a security Intelligence infrastructure so you can
  – Assess the level of risk
  – Justify for your investment in Security
  – Effective monitor and address your vulnerabilities
  – Meet Compliance through Security Intelligence and not think you are secure because you are compliant
Thank you

• Niel.Pandya@oracle.com