Data Privacy - Competing with Identity Thieves: Are You Ready?
Welcome to Today’s Webinar

• Before We Begin
  – CPE Requirements
  – Demographic Polling Question
  – Q&A Session
  – Our Presenter

• Copyright: These materials are presented jointly by The IIA and Deloitte. Use without expressed written permission of is prohibited.
Demographic Polling Questions

1. How many viewers are watching the Webinar at your location?
   a) 1 – I am the only viewer
   b) 2 to 4 viewers
   c) 5 to 7 viewers
   d) 8 to 10 viewers
   e) More than 10 viewers

2. At what level in your internal audit career are you?
   a) New to internal audit
   b) Staff Auditor
   c) Sr. Staff Auditor
   d) Audit Manager
   e) Audit Director
   f) Chief Audit Executive
Webinar Participation

• Submitting Questions to the Presenter:
  – Type the question into the Q&A panel section.
  – Select the “Send” button.
  – We will have a dedicated question and answer session at the end of the presentation to address your questions.

• Technical Assistance
  – Type your issue into the Chat panel section.
  – Select the “Send” button.
  – We will respond to your question privately.
Data Privacy: Competing with Identity Thieves

Mark Steinhoff, Director, Security & Privacy Services
TJ Parks, Senior Manager, Security & Privacy Services
Dan Hoye, Manager, Security & Privacy Services

Deloitte & Touche LLP
Presenters

Mark Steinhoff  
Director  
Security & Privacy Services  
Deloitte & Touche LLP  
msteinhoff@deloitte.com  
+ 1 617 437 2614

TJ Parks  
Senior Manager  
Security & Privacy Services  
Deloitte & Touche LLP  
tjparks@deloitte.com  
+ 1 973 602 6574

Dan Hoye  
Manager  
Security & Privacy Services  
Deloitte & Touche LLP  
dhoye@deloitte.com  
+ 1 617 437 3528
Webinar Objectives

- Discuss the data breach landscape including breach impacts and market drivers/challenges faced in protecting personal data
- Cite the main differences among regulatory requirements in various regions around the globe and consequences for violating international privacy law
- Discuss the privacy legislation around the world, including US, Europe, Canada, Japan, and APEC
- Outline topical areas that may be considered in integrating privacy into the Internal Audit plan
Agenda

• Introduction
• The data breach landscape
• Privacy and data protection overview
• The regulatory landscape
• Integrating privacy into the Internal Audit plan
• Identity theft techniques and controls to prevent/detect
• Useful resources
The data breach landscape
Recent examples of data breaches

Network Solutions breach exposes nearly 600,000
July 27, 2009

The Attorney General of Texas filed a complaint against a pharmacy for illegally disposing of personal information including active debit and credit card numbers, medical prescription forms with customer’s name, address, date of birth, issuing physician and the types of medication prescribed.

Theft of two company laptops containing personal information of 950 people in May

Express Scripts data breach may have hit 700,000 victims
October 1, 2009

Laptop Stolen With Personal Data On 300,000 Health Insurance Clients
January 5, 2008

GatewayCDI, which operates the Mozilla Store, suffered a security breach affecting an undisclosed number of customers
August 5, 2009

Lost Computer Tapes Had Details on 135,000 Workers, Patients
February 8, 2007
Data breaches are on the rise…

• “More electronic records were exposed in 2008 than in the previous four years combined and most of those breaches -- nine out of 10 -- could have been easily avoided with basic preventative controls consistently applied.”

• “91% of all compromised records were linked to organized criminal groups; customized malware attacks doubled; and the most common attack vectors were default credentials and SQL injection.”

• “Verizon…analyzed 90 confirmed breaches that occurred in 2008, affecting 285 million compromised records.”

Source: http://www.informationweek.com: “More Data Breached in 2008 Than in Previous Four Years Combined” April 15, 2009

The data breach landscape is under constant evolution

Numerous instances of data breaches have led to increased awareness at senior executive levels across industries.

Data breaches are common across all sectors.

Source: [www.privacyrights.org/ar/ChronDataBreaches.htm#2008](http://www.privacyrights.org/ar/ChronDataBreaches.htm#2008), Data until 8/22/2008 from Identity Theft Resource Centre

* Ponemon Institute LLC, 2009 Annual Study: U.S. Enterprise Encryption Trends
Impacts of data breaches

A breach could impact many aspects of your business

**Financial Impact**

**Initial Impact**
- 10% of records compromised would result in approximately $2M remediation cost (per incident)
  - Average of $202 of remediation cost per record ($6.6M per breach)

**Ongoing Costs**
- Compliance with multiple regulatory requirements
- Cost of compliance with intrusive regulatory enforcement requirements (e.g., recurring audits for 20 years)
- Cost of fines for non-compliance
- Cost of litigation and class action suits

*Ponemon Institute LLC, 2008 Annual Study: U.S. Costs of a Data Breach*
Impacts of data breaches

A breach could impact many aspects of your business

**Additional Impact**

- Damage to public trust and brand image when data breaches are publicly reported
- Damage to relationships with customers
- Low employee morale
- Productivity loss in responding to regulator inquiries and reporting requirements

*Ponemon Institute LLC, 2008 Annual Study: U.S. Costs of a Data Breach*
## Market drivers and challenges

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Recent media publicity and public awareness on Identity Theft has</td>
<td>• Failure to protect information</td>
</tr>
<tr>
<td>raised the bar significantly</td>
<td>• Inability to accurately manage mobile</td>
</tr>
<tr>
<td>• Regulations and standards such as PCI DSS, HITECH Act, Red Flags</td>
<td>devices and other assets (e.g., PDAs; cell</td>
</tr>
<tr>
<td>and other Federal and statutory regulations with more stringent and</td>
<td>phones; USB drives)</td>
</tr>
<tr>
<td>unambiguous requirements compared to preceding statutory and Federal</td>
<td>• Segregation of duties and access to personal</td>
</tr>
<tr>
<td>requirements</td>
<td>data</td>
</tr>
<tr>
<td></td>
<td>• Difficulty in implementing a comprehensive</td>
</tr>
<tr>
<td></td>
<td>data security/privacy program</td>
</tr>
<tr>
<td></td>
<td>• Balancing legal and compliance requirements</td>
</tr>
<tr>
<td></td>
<td>with operational drivers (e.g., R&amp;D, Marketing)</td>
</tr>
</tbody>
</table>
## Common privacy & data protection challenges

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategy</strong></td>
<td>Complexities about what entities should/should not do with respect to data governance</td>
</tr>
<tr>
<td><strong>Requirements</strong></td>
<td>A myriad of requirements: brand, competitive, regulatory, contractual, ethical, and policy</td>
</tr>
<tr>
<td><strong>Dependencies</strong></td>
<td>Dependencies among entity functions such as security, strategy, HR, compliance, legal, etc.</td>
</tr>
<tr>
<td><strong>Service Providers</strong></td>
<td>Organizations are responsible for their data including data at service providers</td>
</tr>
<tr>
<td><strong>Customization</strong></td>
<td>Generic answers don’t work, response needs to be tailored to the entity’s environment, data and risk</td>
</tr>
<tr>
<td><strong>Impacted by Change</strong></td>
<td>As strategy, processes, systems, and regulations change, privacy controls will need to change as well</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Privacy and security have a paradoxical (symbiotic and antagonistic) relationship.</td>
</tr>
</tbody>
</table>
Common disconnects

“Disconnects” between corporate policies, actual operational practices and technology infrastructure reduces ability to adequately control the protection of information and implement changes into the business environment.
Data should be protected in all phases of the lifecycle

• Data is both an asset and a liability.

• As organizations grow, the volume and complexity of data increases to support the business.

• There are certain types of data (e.g. Personal Information – PI, Protected Health Information – PHI) that must be protected against theft, loss, and misuse. Referred to herein as “information” or “data.”
Polling Question # 1

Why is a common security/privacy challenge faced in the industry today?

a) Segregation of duties and user access
b) Disconnects between policies and processes
c) Interdependencies among business functions
d) All of the above
Privacy and data protection overview
Regional differences

- Despite the similarities that exist amongst various privacy models, there are fundamental regional differences that exist in the world today.

* U.S.*

The prevailing concept is that once an individual provides PII to an organization, the organization becomes the data owner.

Baring any sector-specific privacy legislation, the organization can determine the use of that information.

* EU*

The prevailing concept is that the individual data subject retains rights in his/her PII.

The organization has the responsibilities of a custodian for protecting that PII and using it only in accordance with the rights conveyed by the individual.

* APEC *

The prevailing concept is accountability. Organizations must design privacy protections to prevent harm to individuals from wrongful collection or misuse.

The organization is accountable and obligated to exercise due diligence.
Market requirements

- Enterprises are responding to market requirements for protecting information from insider threats and information leaks.
- Organizations that manage social security numbers, credit card numbers, and patient health information must implement protection measures.
- Financial institutions must protect their consumers from fraud and identity theft.
- Loss of confidential information can result in compliance infractions, lawsuits from customer and/or patients, potential identity theft, and significant harm to an organization’s credibility and reputation.
- Nearly one-third of consumers terminate their relationship with an organization following a security breach.*

What you and your clients want to avoid

<table>
<thead>
<tr>
<th>Delays to Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>• French and German data protection authorities refused to authorise or have suspended projects due to concerns over cross border transfers of employee data</td>
</tr>
<tr>
<td>• Popular fast food chain plans to implement global whistle-blowing schemes were suspended due to privacy and social law concerns raising questions over their compliance with US Sarbanes-Oxley requirements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Restrictions on Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A company was required to process the data of certain employees within the EU after failing to obtain staff consent and provide adequate privacy controls when transferring data to a US-based HR application</td>
</tr>
<tr>
<td>• Italian authorities issued a ‘data processing block’ against a business preventing it from sending any further unsolicited communications because of its failure to put in place appropriate notice and consent requirements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legal Claims and Class Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A company faced the threat of legal action under the UK Data Protection Act 1998 for transferring personal data to call centers in India</td>
</tr>
<tr>
<td>• A large bank paid compensation of £130,000 for accidentally disclosing data of UK credit card customers</td>
</tr>
</tbody>
</table>
What you and your clients want to avoid

Reputational Damage

- A company’s loss of a laptop containing customer information (and their delay in informing those affected by the breach) was widely reported in the UK press in 2006, increasing customer fears around identity theft. This led to an FSA investigation and fines levied of £980,000 ($1.9 million)

Regulatory Sanctions

- A company paid $10 million in civil penalties and $5 million for consumer redress for disclosing sensitive financial information
- A global software company was fined $57,000 for improperly transferring EU employee data to US web server, and was prevented from continuing the transfer of that data
- A company was fined more than €840,000 for failing to enforce customers marketing preferences
Consequences

- Organizations that do not adequately manage the risk of non-compliance with privacy laws and regulations may face the following:
  - Brand damage
  - Compliance with intrusive enforcement requirements
  - Loss of shareholder value
  - Violation of local laws
    - Fines
    - Confiscation of “means to commit the offense” (databases)
    - Criminal penalties for entities and individuals
    - Private lawsuits brought by individual customers, groups of customers or online visitors
  - Loss of confidence with data protection authorities
  - Joint and several liability for supplier failures (EU)
  - Stoppages/delays imposed by regulatory bodies such as Data Protection Authorities (DPAs), Department of Commerce, FTC, and others
  - Potential additional legislation or regulations that will impose greater restrictions
The regulatory landscape
Regulatory requirements

What are governments trying to accomplish?

Goals:
– Address specific issues and threats (e.g., identity theft, spam, selling of PI)
– Protect an individual’s right to exercise control over PI, and what decisions are made with that information
– Protect markets (movement of information across borders)

Methods:
– Articulate data subject rights
– Impose responsibilities on data owners, controllers & processors
– Provide tools to data subjects, regulatory oversight, and enforcement mechanisms

Approaches vary:
– EU omnibus approach applies to personal data processing generally
– US industry sector approach includes targeted privacy provisions in diverse laws
– APEC approach is that the personal information controller must design privacy protections to prevent harm to individuals from wrongful collection or misuse
Commonalities – Fair Information Practices

• 8 fundamental principles of most data privacy requirements:
  • Information collection limitation
  • Data quality
  • Purpose specification/Notice
  • Use limitation
  • Security
  • Openness
  • Individual participation/Access
  • Accountability
EU Data Protection Directive

Through the Data Protection Directive (DPD), the European Union:

- recognizes privacy as a fundamental human right
- established a comprehensive legal framework aimed at protecting individuals and promoting choice regarding the processing of PII
- restricts the movement of PII to only those jurisdictions that provide adequate protection

The EU establishes a unique governing structure
- European Commission
- Working Groups
- Data Protection Authorities
  - At both state and local levels
  - Have business/regulatory and technical arms
- Data Protection Officers
EU Data Protection Directive

- The DPD is a legal and enforceable instrument and governs the transfer and use of PII
- The DPD allows PII to be freely transferred within the European Economic Area (“EEA”), as EEA countries* are already implementing the DPD
- Transfers of PII to countries outside of the EEA are generally prohibited unless the laws of the recipient country offer “adequate protection”
  - The US is deemed to NOT offer “adequate protection”
  - The only countries deemed to provide adequate protection thus far are: Argentina, Canada, Guernsey, Isle of Man, and Switzerland

* EEA countries include: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Republic of Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden and the UK.
Non-EEA data transfers: options

• Safe Harbor
  – EEA to US only; self certification required

• Model Contracts
  – Contractual agreements complaint with EU DPD

• Employee Consent

• Binding Corporate Rules
  – Covers transfers within Corporate group

• Authorization by National Data Protection Authorities
Other International requirements

• Asia-Pacific Economic Cooperation (APEC)
  • Approved by member ministers in November 2004
  • Not in itself international law
  • The framework provides guidance for the development of member country legislation that fosters responsible multi-national data flows in a business friendly environment*

*The APEC member countries include: Australia, Brunei, Darussalam, Canada, Chile, People’s Republic of China, Hong Kong China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, The Russian Federation, Singapore, Chinese Taipei, Thailand, United States, Viet Nam
Other International requirements

• Canada PIPEDA Principles
  • Personal Information Protection and Electronic Documents Act (PIPEDA) requires Canadian organizations to follow a code for the protection of personal information which is guided by 10 Privacy Principles
  • Not in itself international law
• There are also provincial Canada laws in British Columbia and Quebec
Other International requirements

• Japan PIPA Principles

  • Personal Information Protection Act (PIPA) requires Japanese organizations to meet certain requirements for the protection of personal information

  • PIPA requires business to gain individual’s consent to transfer his/her PI to a third party unless one of a narrow set of circumstances exists
United States

Privacy related laws and regulations in the US:

- Typically event driven (something happened in the market)
- Doesn’t necessarily address privacy (but many times aimed at the sale of information)
- Two primary components (usage and security/safeguarding)
- Targeted at particular types of personal information and types of customers
US Federal regulations and governing bodies

- Financial Services Industry
  - Fair Credit Reporting Act (FCRA)
    - FTC, State AG, private right to action
  - Gramm-Leach-Bliley Act (GLBA)
    - FTC, State AG, FS regulators

- Healthcare Industry
  - HIPAA/HITECH Act
    - Department of Health & Human Services (DHHS)
US Federal regulations and governing bodies

- Consumer Business Industry
  - Deceptive Trade Practices (sect 5)
    - FTC, State AG
  - The Children’s Online Privacy Protection Act of 1998 (COPPA)
    - FTC, State AG
  - Payment Card Industry Data Security Standard (PCI DSS)
    - Payment card brands (e.g. Visa, AMEX)
US Federal regulations and governing bodies

• All Industries
  • Red Flag Rules
    • FTC, State AG
  • Workplace privacy
    • State AG; EEOC
Statutory breach notification laws

• Driven by Breach Notification Laws in nearly all states, breach notification requirements expose businesses to potentially significant losses arising from:
  - Negative publicity
  - Loss of reputation
  - Regulatory fines
  - Class action lawsuits

• Organizations have been significantly impacted by the increase in regulatory and industry requirements to report breaches of PI to data subjects or business partners.
Statutory breach notification laws

• Common requirements:
  • Require notification to affected individuals of unauthorized PI access
  • Disclosure requirements are triggered when individual/business knows or reasonably believes there has been a security breach
  • A security breach typically means unauthorized acquisition of unencrypted PI
  • If an security breach is discovered, residents must be notified in the "most expedient time possible" without unreasonable delay
  • Notice may be delayed if it would impede a criminal investigation or to allow a company to determine the extent of the breach and take action to restore security
Statutory breach notification laws

- Key Outliers:
  - AR, DE, IN, NV, ND, and NY include either medical, last 4 SSN, employer ID, mother’s maiden name, signature, or biometric data
  - AR, NV, and TX require reasonable security measures. Encrypted data is does not appear to be exempt in NY and MN.
  - AR, MT, NV, NYC, and TX impose a duty of secure destruction
  - In NV, businesses may not transfer covered data without encryption unless internally or by facsimile effective 10/1/08
Polling Question # 2

Which of the following statements is true?

a) Breach notification is governed by Federal law
b) Every state has different breach notification requirements
c) Breach notification requires the notification of unauthorized use or disclosure of PI to the affected individuals
d) Safe Harbor certification means that you do not have to abide by breach notification requirements
Statutory breach notification laws – trend setter

• CA SB 1386 – “Personal Information” refers to an individual's first name or first initial and last name, in combination with any of the following (if the information is unencrypted):
  • SSN; drivers licenses or ID card number
  • Account number, credit/debit card number, in combination with a required security code, access code, or password that would permit access to an individual’s financial account
  • Medical or health insurance information
Emerging US statutory regulations

• MA 201 CMR 17.00 – Standards for the Protection of PI of Residents of the Commonwealth
  • Effective March 1, 2010
  • Requires every person/company who owns or licenses MA resident PI must implement a written security program covering the provisions within the regulation

• Outlines specific provisions for:
  • program ownership;
  • risk assessment and incident response;
  • training and awareness programs
  • encryption;
  • service providers;
  • security controls for computer systems;
  • among others
Emerging US statutory regulations

• Nevada NRS 597.970 – Restrictions on Transfer of PI Through Electronic Transmission
  • Effective October 1, 2008
  • Requires businesses in the state of Nevada to encrypt PI in transit

• New Jersey STAT. § 56:8-161
  • Effective April 7, 2008
  • Requires proper disposal of records containing PI to ensure no unauthorized access to that information
  • Includes SSN protections
Emerging US statutory regulations

- Connecticut H.B. 5658 – An Act Concerning the Confidentiality of SSN
  - Effective October 1, 2008
  - Requires safeguarding of PI from misuse by third parties and proper disposal of PI
  - Requires an organization to develop and implement SSN privacy policy, which must:
    - Protect confidentiality of SSNs
    - Prohibit unlawful disclosure of SSNs
    - Limit access to SSNs
SSN protection

- Use, disclosure, and protection of SSNs
  - 26 states have enacted legislation restricting the use/disclosure of SSNs and require SSN safeguards
  - 47 states have enacted Identify Security Freeze Laws to help prevent unauthorized use of consumer report information to fraudulently open a new account
Polling Question # 3

What is one main difference between US and European privacy laws?

a) Privacy is a fundamental human right based on the US constitution
b) European laws recognize privacy as a fundamental human right
c) Europe does not have laws governing the protection of PI
d) There is no difference between US and European privacy laws
Regulatory pressure

Organizations not only have to protect their data, but also have to comply with regulations with overlapping and duplicative requirements.

“One off” approach creates multiple discrete compliance programs which leads to inconsistency and inefficiency in managing requirements from multiple regulations.
Regulatory landscape management

• It is imperative to take a holistic approach to perform these assessments especially when the organization is subject to multiple regulations with overlapping, complimentary, and duplicative requirements.

• Your approach may include:
  • assessing the commonalities (e.g. user access controls) and differences (e.g. data covered in scope) among regulatory requirements
  • determining which provisions should be implemented at the corporate level versus the local level to drive efficiencies through the process.
Integrating privacy into the Internal Audit plan
Risk assessment

- Incorporate security and privacy risks into the company risk assessment process
  - Regulatory risks
    - what regulations affect your company?
    - are you compliant?
  - Technology risks
    - system vulnerabilities, access to PI, etc
  - Operational risks
    - where is PI at your company?
    - how is it protected?
Risk assessment (cont)

- Identify the varying requirements of applicable regulations
  - What is common/different among regulations?
    - Technology requirements
    - Breach notification requirements
    - Governing bodies
  - What information is in scope (e.g. PI, PHI, employee data, customer data, domestic, international…)
  - What provisions can be centralized?
Incident response

- Validate that an incident response plan is in place to guide personnel in the efficient handling of security breaches
  - Escalations procedures
  - Aligned with applicable regulations
    - e.g. includes breach notification requirements
  - Post-incident/root cause analysis
  - Implementation of corrective action
Security/Privacy policies and programs

• Validate that up to date policies/programs exist at your company for:
  • Compliance with applicable regulations
  • Protection of PI records (logical/physical)
  • Identification/Classification of records
  • Records Retention/Information Management
  • Disciplinary measures for non-compliance
  • Periodic reviews of policies

• Is accountability/ownership defined?
Training and awareness

• Validate that training and awareness programs exist to educate personnel on:
  • Policies and procedures in place
  • The handling of PI
  • Requirements/differences of applicable regulations

• Validate that attendance to training and awareness for required trainings is monitored
Service providers

• Understand what third party service providers are transferring or receiving PI on the company’s behalf:
  • Are contracts in place? Do contracts have privacy related language?
  • Is there a process in place to review contracts for compliance with applicable regulations?
  • Is PI secure in transit and in the third party’s possession?
  • Is PI transferring across borders?
Appropriate controls

- Validate that controls are in place to protect the unauthorized use or disclosure of PI:
  - Logical/physical access
  - Encryption
  - Activity monitoring (user/network)
  - Up to date IDS/IPS/Firewalls
  - Up to date anti-virus
Overall integration

- When dealing with multiple regulations, sometimes the most efficient and effective way to develop consistent policies, procedures, and controls is to address the common provisions among applicable regulations.

- Specific provisions can be addressed on an as-needed basis.
Polling Question # 4

What should you consider as your first step in implementing a privacy program?

a) Implement a training and awareness program for all employees
b) Implement an encryption solution to protect all company data
c) Perform a risk assessment
d) Decide if your company needs a privacy program
Identity Theft techniques and controls to prevent/detect
Some common techniques

- **Hacking**
  - External threats such as SQL injection, cross-site scripting, phishing, password cracking, botnet attacks, etc

- **Malware**
  - Spyware, worms, backdoors, trojan horses, viruses

- **Social engineering**
  - Influencing people to divulge information such as passwords, personal information, etc

- **Human error/misuse**
  - Employee/third party abuse of access privileges
  - Employees placing unauthorized software on systems

- **Loss/Theft of information**
  - Loss or theft of laptops, backup tapes, USB drives, PDAs, etc containing information
What are some examples of controls?

<table>
<thead>
<tr>
<th>Technique</th>
<th>Safeguard Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking</td>
<td>• Intrusion detection/prevention systems</td>
</tr>
<tr>
<td></td>
<td>• Control over “privileged” access to systems</td>
</tr>
<tr>
<td></td>
<td>• Activity logging and monitoring</td>
</tr>
<tr>
<td></td>
<td>• Encryption of data in motion and at rest</td>
</tr>
<tr>
<td>Malware</td>
<td>• Up to date antivirus software and definitions</td>
</tr>
<tr>
<td></td>
<td>• Frequent updating of antivirus software</td>
</tr>
<tr>
<td></td>
<td>• Preventing users from installing software on company resources</td>
</tr>
<tr>
<td></td>
<td>• Activity logging and monitoring</td>
</tr>
<tr>
<td></td>
<td>• Email filtering</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>• Policies for information sharing and escalation procedures</td>
</tr>
<tr>
<td></td>
<td>• Employee training and awareness programs</td>
</tr>
</tbody>
</table>
What are some examples of controls?

<table>
<thead>
<tr>
<th>Technique</th>
<th>Safeguard Examples</th>
</tr>
</thead>
</table>
| Human error/ misuse     | • Controls over access to systems and resources (e.g. least privilege)  
                           • Employee training and awareness programs  
                           • Monitoring of access to logical/physical records  
                           • Encryption of data in motion and at rest |
| Loss/Theft of information | • Policies for acceptable use and handling of company assets  
                              • Background checks for personnel and third parties  
                              • User de-provisioning controls including immediate removal of physical, network, and high-risk system access  
                              • Monitoring of access to logical/physical records  
                              • Employee training and awareness programs  
                              • Encryption of data in motion and at rest |
Polling Question # 5

Which of the below is not a technique used for identify theft?

a) Social engineering
b) Phishing
c) Stealing a backup tape
d) .jpeg projection
Useful Resources
Useful Resources


Useful Resources

• The People Dimension of Security and Privacy: Eight Training and Awareness Habits of Highly Effective Organizations
Useful Resources

_Combating Cyber-Threats from the Underground Economy: A View from the Front Lines_

- Dbriefs Webcast (w/CPE) focuses on cyber-crime in the world today and its ever-evolving sophistication
- Discusses the following topics:
  - The cyber-threat industry, including supply chains, monetization of electronic theft, and the competitive marketplace of stolen information
  - The evolution of cyber-crime from smash-and-grab technologies to parasitic strains operating below the pain threshold
  - Predictive data security strategies including adapting to evolving cyber-threats and protection the enterprise while still adhering to privacy and labor laws
- DATE: December 3, 2009 @ 1pm EST
Useful Resources

**Intensive Risk, Elusive Value: A Risk Intelligent Executive’s Guide to Security and Privacy**

- Useful tool for business leaders in their efforts to assess their organization's Risk Intelligence, while enhancing their approach to security and privacy.
- Discusses key security and privacy takeaways along with actionable recommendations, including:
  - Taking a proactive approach to avoid breaches
  - Addressing the associated people issues
  - Realizing the potential of information technology
  - Forging the link between policies and operations
  - Linking security and privacy with strategic business objectives
Useful Resources

The People Dimension of Security and Privacy: Eight Training and Awareness Habits of Highly Effective Organizations

• Offers guidance to increase the efficiencies and effectiveness of a company’s security and privacy training and awareness, including:
  • Ownership and tone at the top
  • Focus on highest risks first
  • Consider a role-based approach
  • Develop ongoing awareness campaigns
  • Make everyone a part of the fortress
  • Measure the results
QUESTIONS?
Contact Information

Mark Steinhoff
Director, Security & Privacy Services
Deloitte & Touche LLP
msteinhoff@deloitte.com
+1 617 437 2614

TJ Parks
Senior Manager, Security & Privacy Services
Deloitte & Touche LLP
tjparks@deloitte.com
+1 973 602 6574

Dan Hoye
Manager, Security & Privacy Services
Deloitte & Touche LLP
dhoye@deloitte.com
+1 617 437 3528
This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.
CPE Certificates

Registered participants who have met the CPE requirements will receive their CPE Certificate by e-mail in approximately one week.
Webinar Playback

• Paid attendees of this live Webinar can access the playback at no cost by contacting our Customer Support Team at +1-407-937-1111.
Upcoming IIA Webinars

• Assessing the Effectiveness of Compliance & Ethic Programs
  – November 05, 2009

• Construction Auditing
  – November 12, 2009

• Spreadsheet Management Strategy: Adding Value While Improving Controls
  – November 19, 2009
IIA Virtual Seminars

- Virtual Seminars are an online version of our traditional seminar courses that offer the same high quality and standard of excellence. Our Virtual Seminars cover the same concepts and materials while utilizing the curriculum and exercises as their traditional counterparts.

- All Virtual Seminars are written and developed by practitioners, for practitioners. We provide the course, you provide the comfy chair. That's right! Study wherever it's the most convenient for you because you can attend any of our Virtual Seminars wherever an Internet connection is available.

To learn more about upcoming classes, visit www.theiia.org/e-learning
Upcoming IIA Virtual Seminars

• Operational Auditing: An Introduction
  – November 2 – 13, 2009

• Risk-based Auditing: A Value Add Proposition
  – November 9 – 20, 2009

• Value Added Business Controls: The Right Way to Manage Risk
  – November 16 – 27, 2009

• Operational Auditing: Advanced
  – November 30 – December 11, 2009