Proudly presents…

3D- Enterprise Best Practices in the Cyber World

Presented by

Eduard Goodman, J.D., LL.M., CIPP-US/C

Chief Privacy Officer

IDT911

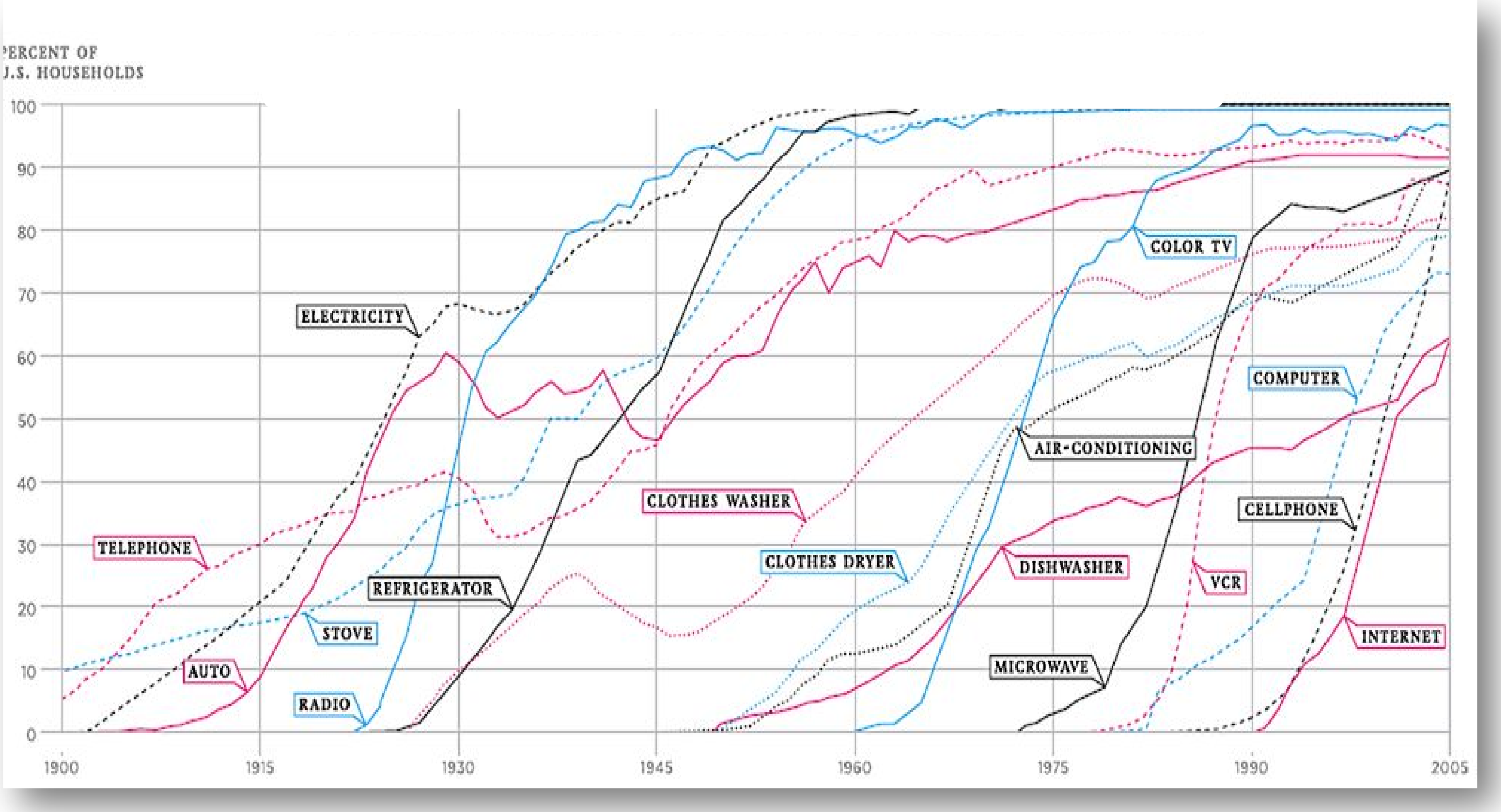
Agenda

- INTRODUCTION AND OVERVIEW- WHY YOU NEED TO INTEGRATE DATA RISK MANAGEMENT INTO ENTERPRISE RISK MANAGEMENT STRATEGIES
- DATA RISK MANAGEMENT EXPLAINED
- THE IMPORTANCE OF INTEGRATING DATA RISK MANAGEMENT INTO OVERALL ENTERPRISE RISK MANAGEMENT
- SUMMARY OF (CANADIAN) REGULATORY ENVIRONMENT
- BEST PRACTICES FOR EFFECTIVE DATA RISK MANAGEMENT
- CONCLUSION -OR- A BETTER UNDERSTANDING OF WHERE TO GO FROM HERE

INTRODUCTION AND OVERVIEW-

WHY YOU NEED TO INTEGRATE DATA RISK MANAGEMENT INTO ENTERPRISE RISK MANAGEMENT STRATEGIES

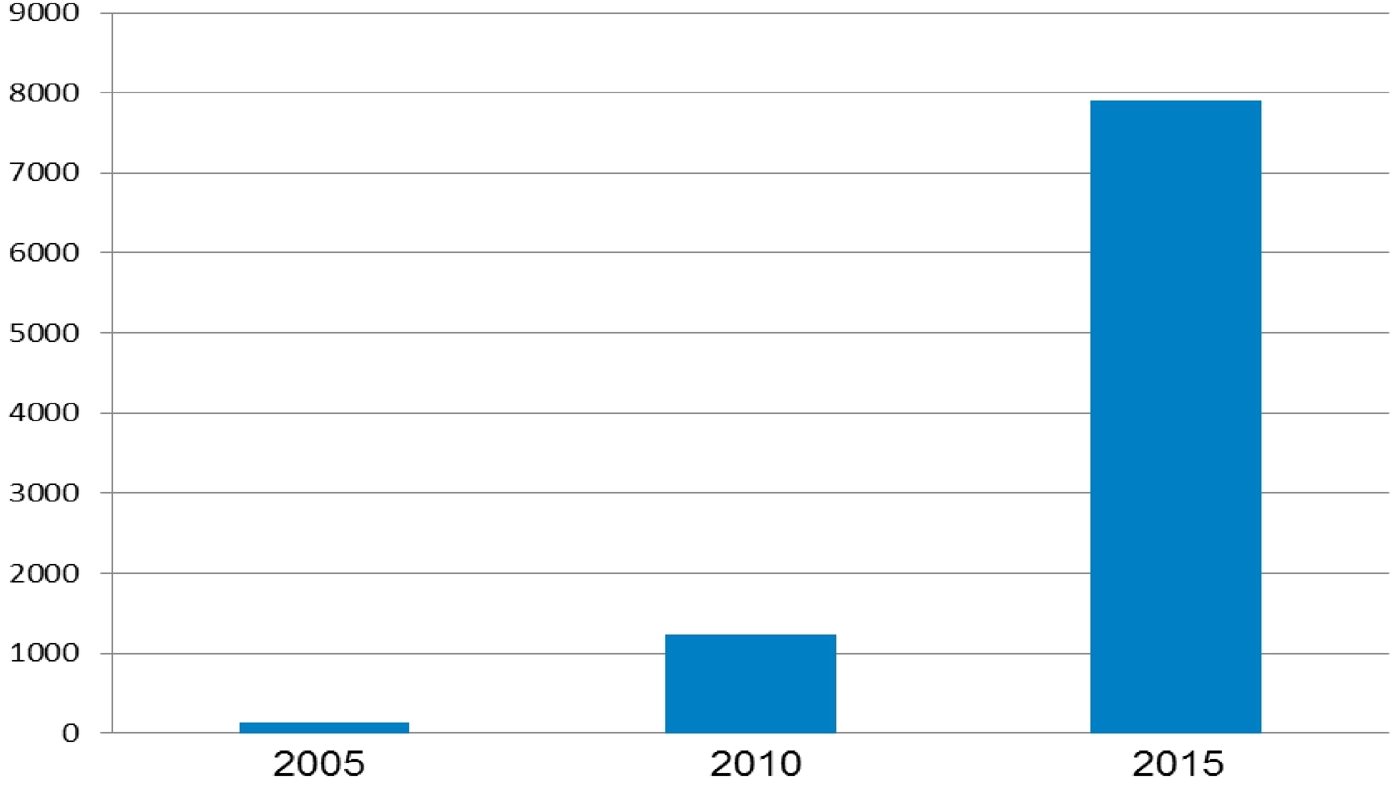
Explosion of information accessibility: Over 60% adopt the internet within 15 years



HORIZONS
2012 RIMS Canada Conference - Saskatoon

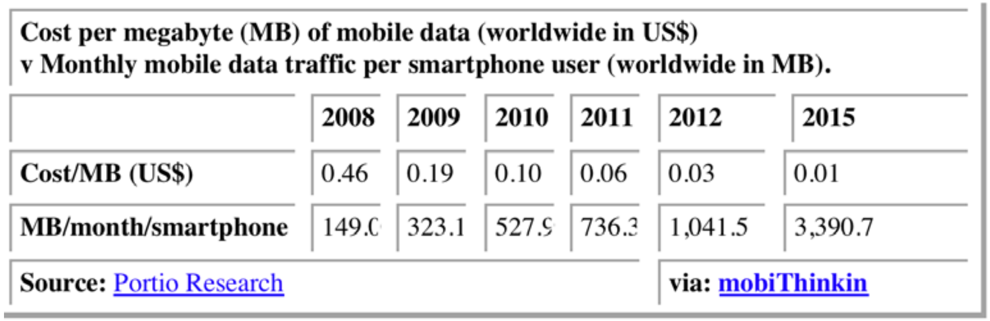
Explosion of information accessibility: Data storage growth

A Decade of Digital Universe Growth: Storage in Exabytes



Source: IDC's Digital Universe Study, sponsored by EMC, June 2011

Explosion of information accessibility: Growth in mobile access to data



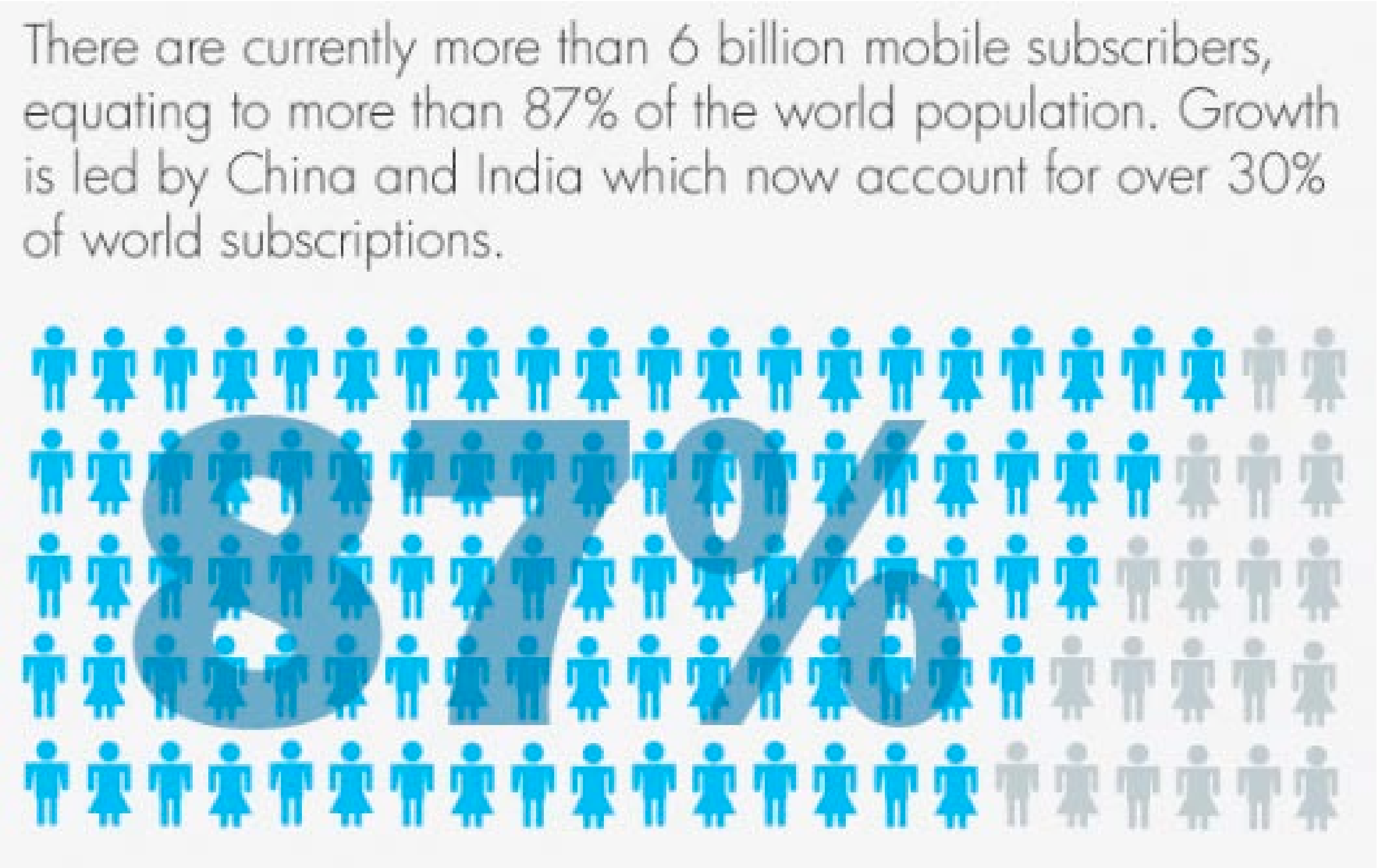
Cost per megabyte (MB) of mobile data (worldwide in US$)
v Monthly mobile data traffic per smartphone user (worldwide in MB).

	2008	2009	2010	2011	2012	2015
Cost/MB (US$)	0.46	0.19	0.10	0.06	0.03	0.01
MB/month/smartphone	149.0	323.1	527.9	736.3	1,041.5	3,390.7

Source: Portio Research | via: mobiThinkin

http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats

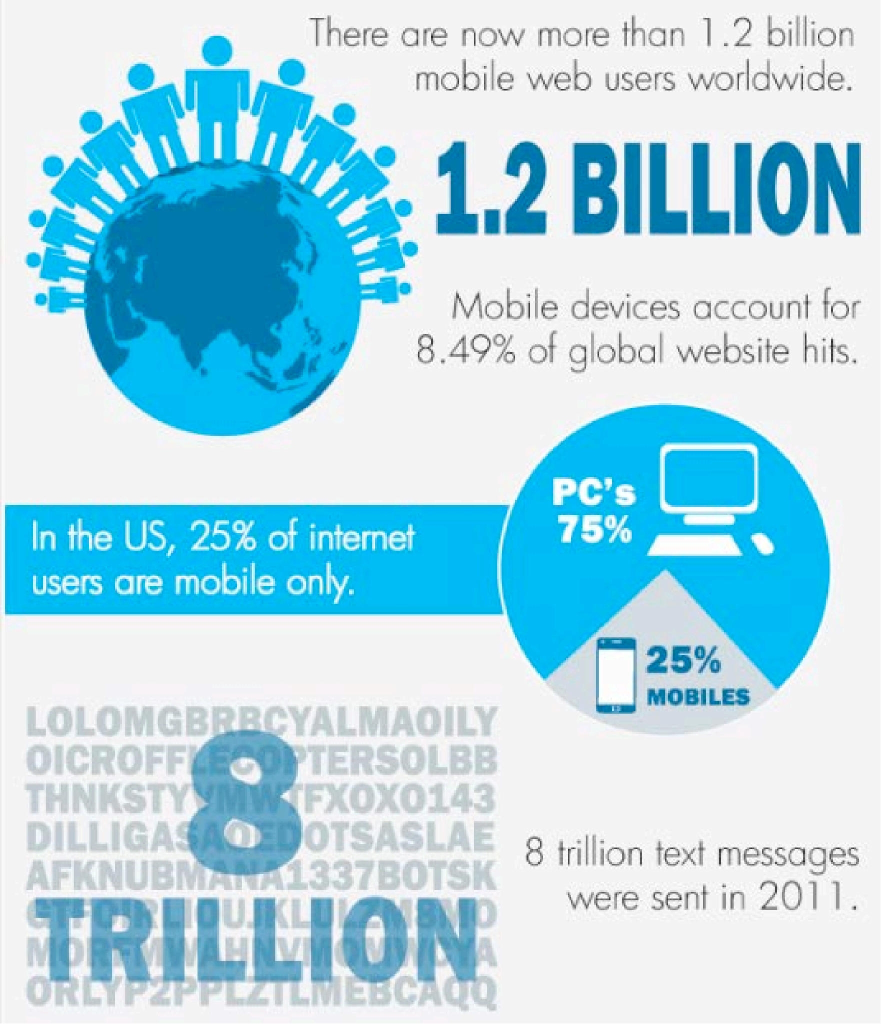
Explosion of information accessibility: Growth in mobile access to data



There are currently more than 6 billion mobile subscribers, equating to more than 87% of the world population. Growth is led by China and India which now account for over 30% of world subscriptions.

http://www.digitalbuzzblog.com/infographic-2012-mobile-growth-statistics/

Explosion of information accessibility: growth in mobile access to data



There are now more than 1.2 billion mobile web users worldwide.

1.2 BILLION

Mobile devices account for 8.49% of global website hits.

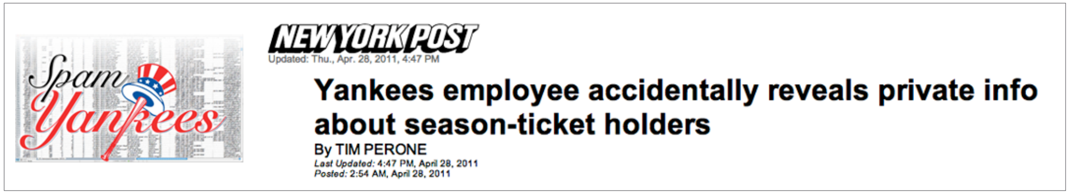
In the US, 25% of internet users are mobile only.

8 TRILLION

8 trillion text messages were sent in 2011.

http://www.digitalbuzzblog.com/infographic-2012-mobile-growth-statistics/

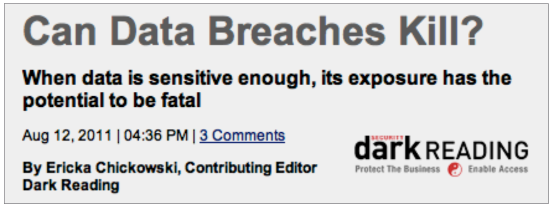
Increases in data storage and accessibility results in increased exposure of information…



NEW YORK POST
Updated: Thu., Apr. 28, 2011, 4:47 PM

Yankees employee accidentally reveals private info about season-ticket holders

By TIM PERONE
Last Updated: 4:47 PM, April 28, 2011
Posted: 2:54 AM, April 28, 2011



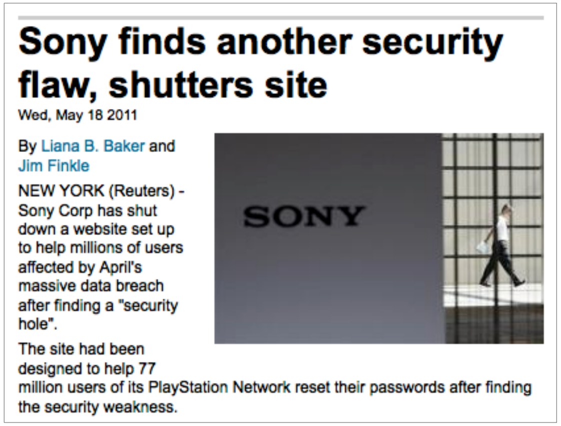
Can Data Breaches Kill?

When data is sensitive enough, its exposure has the potential to be fatal

Aug 12, 2011 | 04:36 PM | 3 Comments

By Ericka Chickowski, Contributing Editor
Dark Reading

SECURITY dark READING
Protect The Business Enable Access



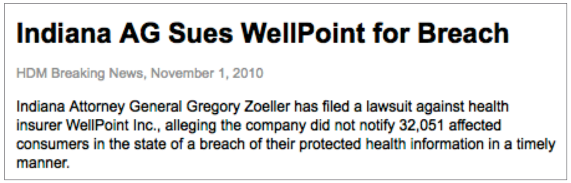
Sony finds another security flaw, shutters site

Wed, May 18 2011

By Liana B. Baker and Jim Finkle

NEW YORK (Reuters) - Sony Corp has shut down a website set up to help millions of users affected by April's massive data breach after finding a "security hole".

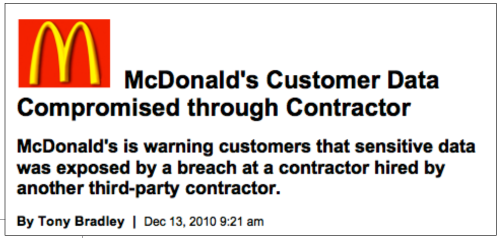
The site had been designed to help 77 million users of its PlayStation Network reset their passwords after finding the security weakness.



Indiana AG Sues WellPoint for Breach

HDM Breaking News, November 1, 2010

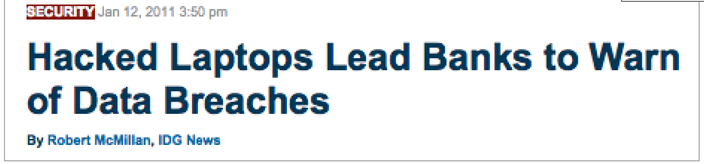
Indiana Attorney General Gregory Zoeller has filed a lawsuit against health insurer WellPoint Inc., alleging the company did not notify 32,051 affected consumers in the state of a breach of their protected health information in a timely manner.



McDonald's Customer Data Compromised through Contractor

McDonald's is warning customers that sensitive data was exposed by a breach at a contractor hired by another third-party contractor.

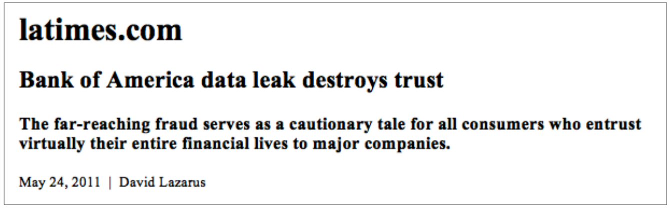
By Tony Bradley | Dec 13, 2010 9:21 am



SECURITY Jan 12, 2011 3:50 pm

Hacked Laptops Lead Banks to Warn of Data Breaches

By Robert McMillan, IDG News

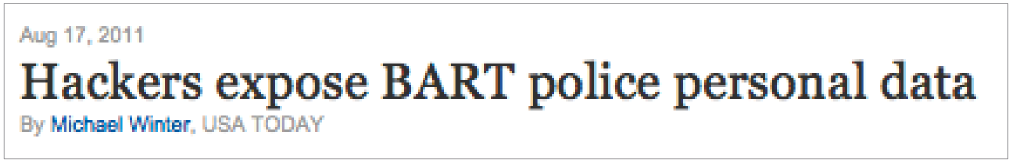


latimes.com

Bank of America data leak destroys trust

The far-reaching fraud serves as a cautionary tale for all consumers who entrust virtually their entire financial lives to major companies.

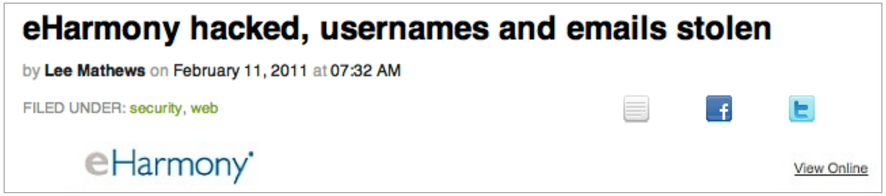
May 24, 2011 | David Lazarus



Aug 17, 2011

Hackers expose BART police personal data

By Michael Winter, USA TODAY



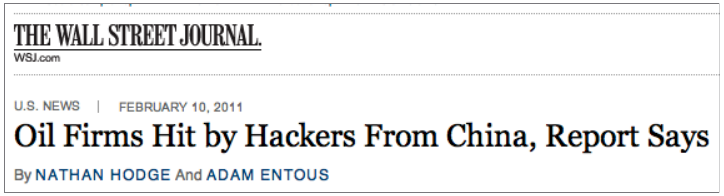
eHarmony hacked, usernames and emails stolen

by **Lee Mathews** on February 11, 2011 at 07:32 AM

FILED UNDER: security, web

eHarmony

View Online



THE WALL STREET JOURNAL.
WSJ.com

U.S. NEWS | FEBRUARY 10, 2011

Oil Firms Hit by Hackers From China, Report Says

By NATHAN HODGE And ADAM ENTOUS

Fraud & Risk Trends-
Privacy at Risk/Information Under Attack

- Consumer and Business Information has become a “Criminal Commodity”
- Information’s value and market for open exchange has increased to unprecedented scale.
- Information has become the currency and enabler of FRAUD

Fraud & Risk Trends-
Privacy at Risk/Information Under Attack

The reason?

- **Information = Transactional Access in the financial services world – and it is all about the MONEY!....but sometimes with "Hacktivists" – It's the Info:**
  - Internal data compromise
  - External data compromise

DATA RISK MANAGEMENT EXPLAINED

What is Data Risk Management

Data risk management assesses a company's protection posture and vulnerabilities to identify potential risks that could result in the compromise of critical data.

What is Data Risk Management

Data risk management then Identifies, Recommends, and Implements:

- policies,
- practices; and
- systems

to mitigate the exposures and minimize the risks.

What is Data Risk Management

Data risk management encompasses the disciplines of:

- data protection;
- privacy;
- compliance;
- information security;
- fraud;
- cyber-crime prevention;
- data event investigation and management; and
- technical assessment and forensics.

What is Data Risk Management

A comprehensive assessment & plan should take a holistic “end-to-end” view of the company with special attention to bridging the “silos” between internal operations.

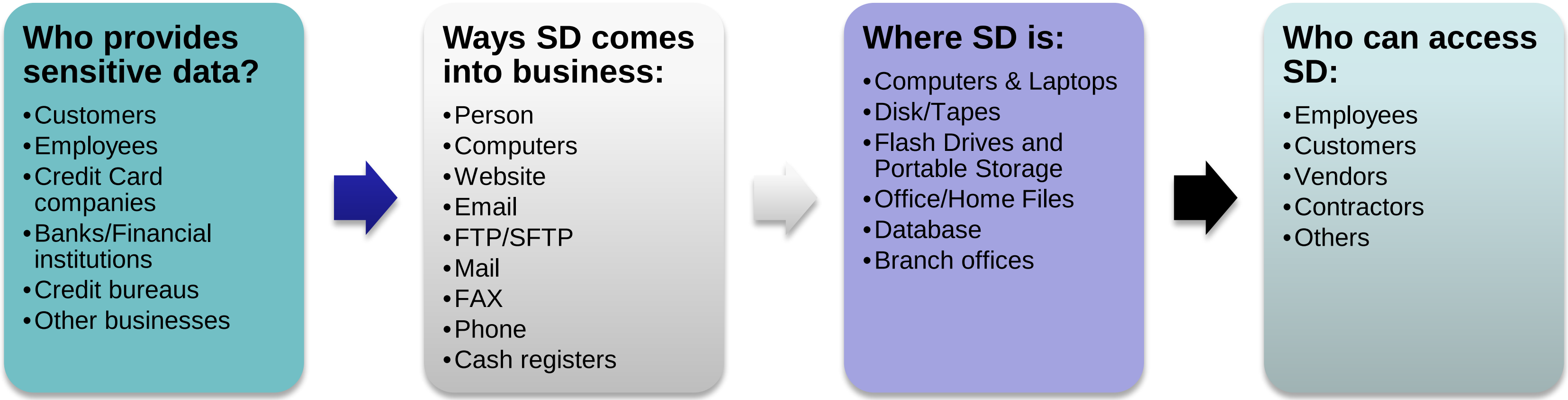
What is Data Risk Management

It is important that the client company and the individuals entrusted with sensitive data clearly understand the different types of data and why it is important to protect this type of data. This includes 3rd parties to whom the data may be provided.

Sensitive data puts a company at risk

How is sensitive data a risk?

Sensitive Data (SD) is a risk because competitors & criminals want it and it gets lost and unintentionally exposed. And, it's difficult to keep track of, because SD comes into, through and out of a business in a number of ways. Different types of information present varying risks. *Consider...*



Who provides sensitive data?

- Customers
- Employees
- Credit Card companies
- Banks/Financial institutions
- Credit bureaus
- Other businesses

Ways SD comes into business:

- Person
- Computers
- Website
- Email
- FTP/SFTP
- Mail
- FAX
- Phone
- Cash registers

Where SD is:

- Computers & Laptops
- Disk/Tapes
- Flash Drives and Portable Storage
- Office/Home Files
- Database
- Branch offices

Who can access SD:

- Employees
- Customers
- Vendors
- Contractors
- Others

THE IMPORTANCE OF INTEGRATING
DATA RISK MANAGEMENT INTO
OVERALL ENTERPRISE RISK MANAGEMENT

So as Risk Managers – Why is topic important?

It’s about awareness, recognition, planning, action & respons…it’s also about passion!

- It impacts you as an individual & your family
- It impacts your company and you in your role as a risk manager
- It impacts your vendors and support resources
- It impacts your customers and clients

So as Risk Managers – Why is topic important?

It can be insidious!

- It's usually "never a problem – until there's a problem"
- As an RM, you are expected to see around the corners and into the future – "How did YOU let this happen?!!"

So as Risk Managers – Why is topic important?

It can be insidious!

- If you are not concerned and looking at the holistic picture including the downside consequences likely no one else is. Silos create blind spots.

- You are the “control evangelist” – Position to being the “go- to” resource for identifying issues AND providing solutions

Welcome to the “Darkside”

Key Tenets of Successful Risk Management

- The “Field of Schemes” – Build it and they will come!

- Recognize that there are people out there that are trying to steal your business/your money from you.

Welcome to the "Darkside"

Key Tenets of Successful Risk Management

CASE STUDY

- ***Hackers Steal, Encrypt Health Records and Hold Data for Ransom***
  - *http://go.bloomberg.com/tech-blog/2012-08-10-hackers-steal-encrypt-health-records-and-hold-data-for-ransom/*

Welcome to the “Darkside”

Key Tenets of Successful Risk Management

- Every Product & Process (and modifications there to) have internal and external theft and risk ramifications as well as operating error exposure that must be balanced with control, detection, and audit capabilities.

Welcome to the “Darkside”

Key Tenets of Successful Risk Management

- We must examine and understand the systems and supporting processes from “end-to-end” to identify potential vulnerabilities.

- We must understand existing and newly emerging threats to the technology – it is a very dynamic and often hostile environment.

Welcome to the “Darkside”

Key Tenets of Successful Risk Management

CASE STUDY

- ***Anatomy of a breach***
  - *http://blogs.rsa.com/rivner/anatomy-of-an-attack/*

Welcome to the “Darkside”

Key Tenets of Successful Risk Management

- Risk Exposure - The Stakes are High! – We need to Control it and “Cap it.” wherever possible.

- What you don’t know can and will hurt you – it’s not a matter of “if” but rather of “when”! – Pay me now or Pay Big Later!”

Welcome to the "Darkside"

Key Tenets of Successful Risk Management

- In the Risk Arena – Don't Look To the Past To Determine the Future – Learn from the past – but don't predict from it.

- Denial & Complacency Kills! – Don't underestimate your adversary, the environment or "Mr. Murphy" …and Luck eventually runs out!

Welcome to the "Darkside"

Key Tenets of Successful Risk Management

CASE STUDY

- ***How Apple and Amazon Security Flaws Led to My Epic Hacking***
  - ***http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/***

Welcome to the “Darkside”

Key Tenets of Successful Risk Management

- Reputational Risks – Strong control and loss prevention postures are key to protection of your products and services – even your “Brand.”

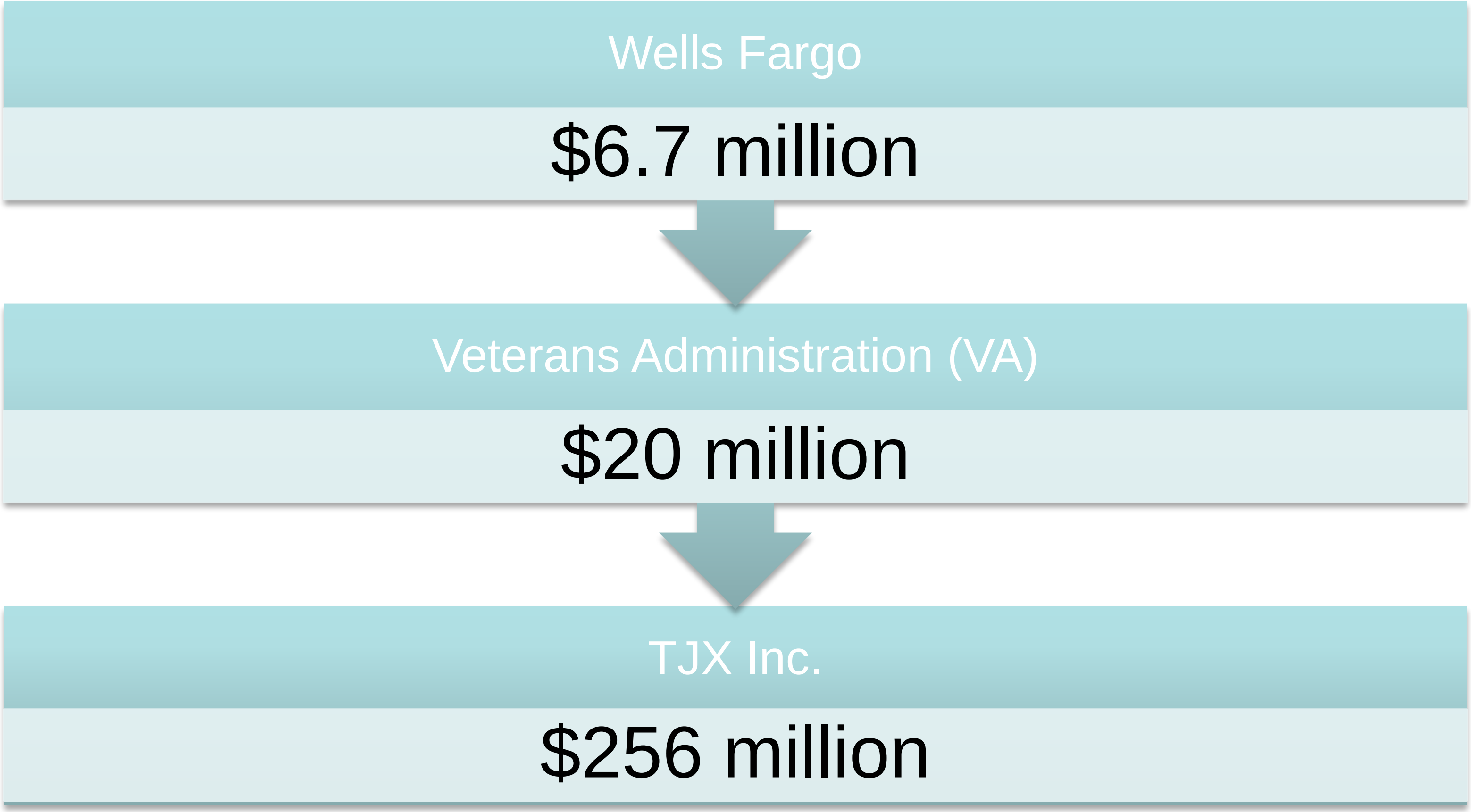
Welcome to the “Darkside”

Key Tenets of Successful Risk Management

- Regulatory Risks – Heavy Emphasis on customer verification, identity theft, customer privacy & authentication

- Litigation Exposures – Some Brave New Worlds out there

Litigation/Settlements (U.S.)



Wells Fargo

$6.7 million

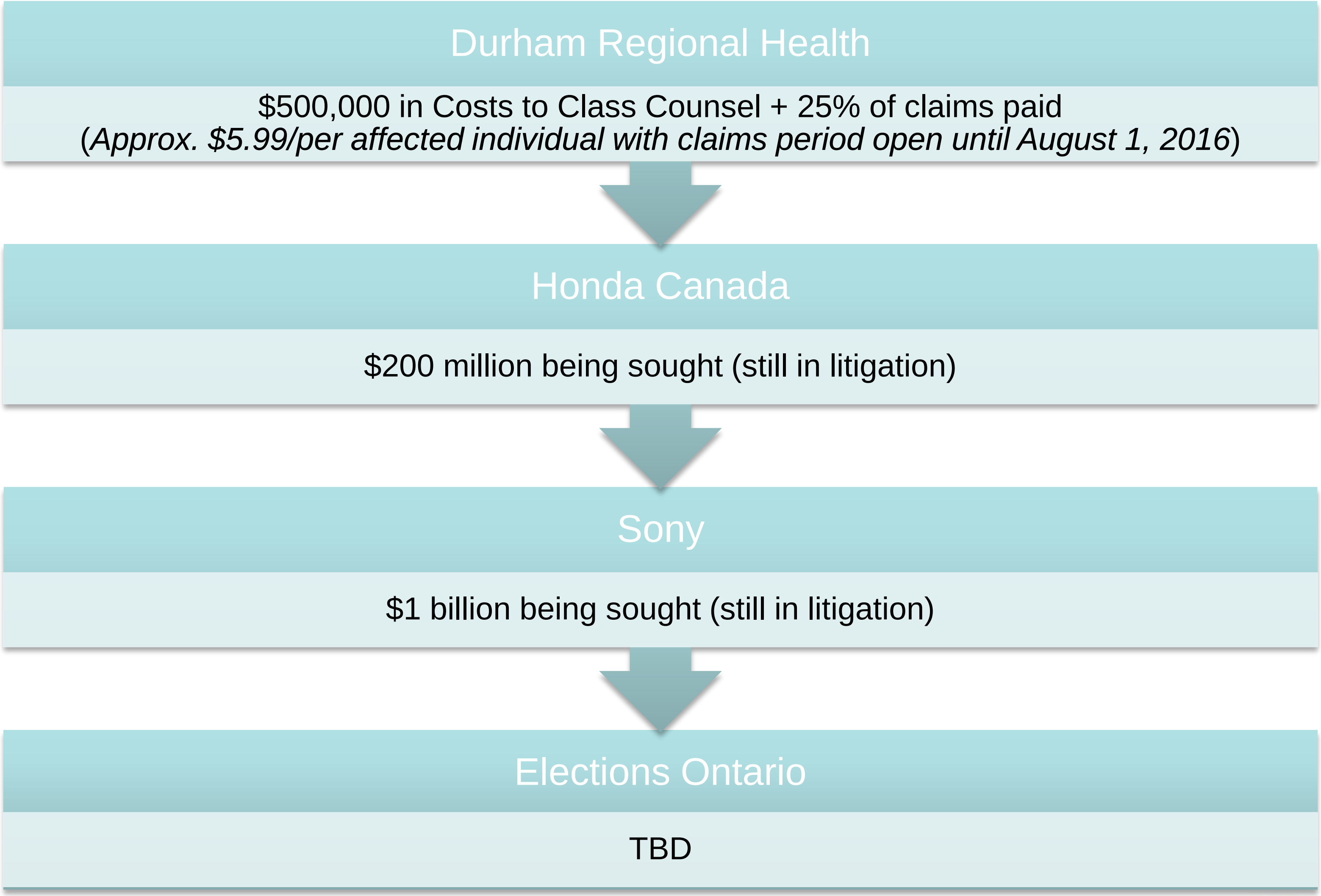
Veterans Administration (VA)

$20 million

TJX Inc.

$256 million

Litigation/Settlements (Canada)



Durham Regional Health

$500,000 in Costs to Class Counsel + 25% of claims paid
(*Approx. $5.99/per affected individual with claims period open until August 1, 2016*)

Honda Canada

$200 million being sought (still in litigation)

Sony

$1 billion being sought (still in litigation)

Elections Ontario

TBD

Prevalent Internet Cyber Schemes:

- Phishing, Pharming, Smishing, Vishing…
- SPAM – Fraudulent Notification or **Requests** for Information – vectors for malware infection
- BOTS & BOTNETS - Purloined computers/networks used for Spam & malware distribution

Prevalent Internet Cyber Schemes:

- Malicious Software – Spyware; Virus Infection; Key Stroke Capture; turn off protections; create cache; backdoors & high value transaction alerting; Zero Day attacks; ZEUSS et al.

- Web Site Impersonations, Spoofing & Redirection – Collection of Account & Authentication Information

Prevalent Internet Cyber Schemes:

- Man in the Middle, Man in the Browser & Session Hijacking

- Breach of Credit Card Processors & Merchant

  sites for theft of customer and account information – followed by fraudulent transactions & card counterfeiting

Prevalent Internet Cyber Schemes:

- Exploitation of Social Networking & Peer to Peer File Share Functions – PTP; BTB; BTP

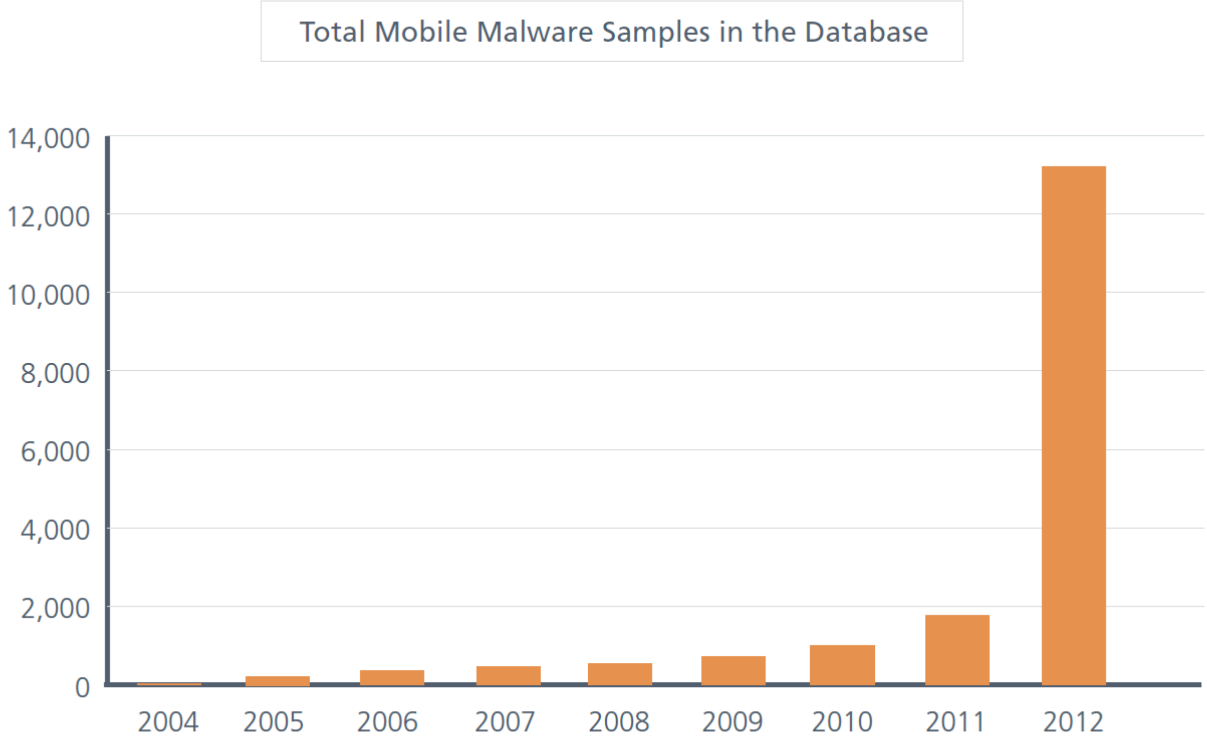
- Identity Theft/Customer Impersonation – Establishment of new account and remote authentication challenges

Prevalent Internet Cyber Schemes:

- Packet Sniffing – customer, employment, transmission site or bank
- Use of remote access PC programs (PC Anywhere/Timbuktu)
- Denial of Service Attacks
- Web Vandalism

New Risk Vectors: Smart Phones

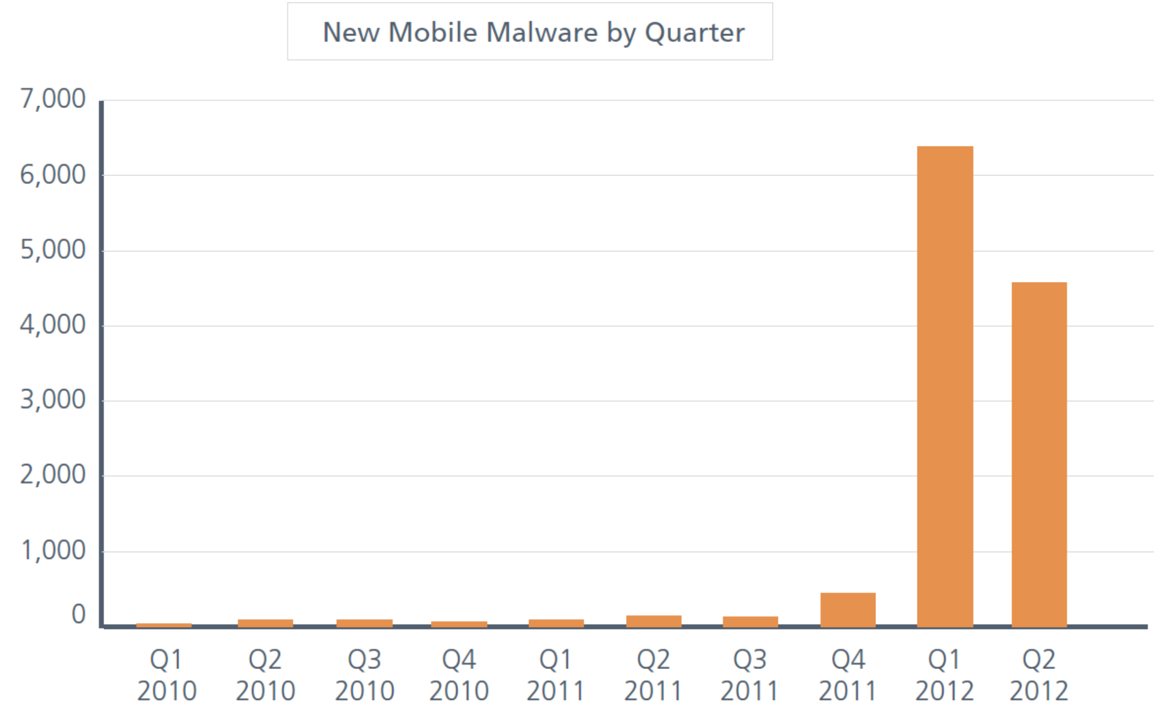
- Increase in Smart Phone based threats is staggering:



McAfee Threats Report: Second Quarter 2012, McAfee Labs, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf.

New Risk Vectors: Smart Phones

- Increase in Smart Phone based threats is staggering:



McAfee Threats Report: Second Quarter 2012, McAfee Labs, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf.

New Risk Vectors: Smart Phones

- The malware sample discovery rate has accelerated to nearly 100,000 per day.

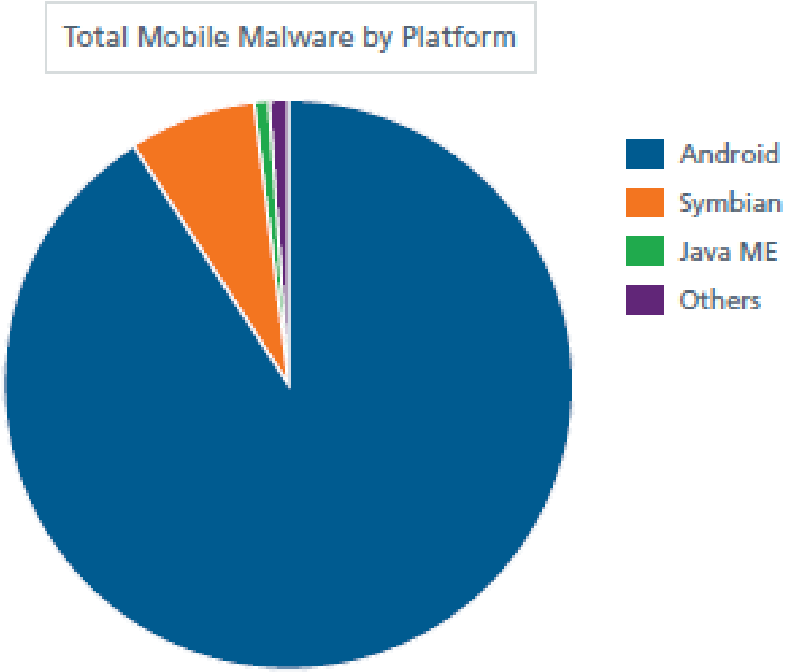
- Stark Increase in Ransomware

- New Mobile controlled Botnets (Twitter based
  mobile command and control

McAfee Threats Report: Second Quarter 2012, McAfee Labs,
http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf.

New Risk Vectors: Smart Phones

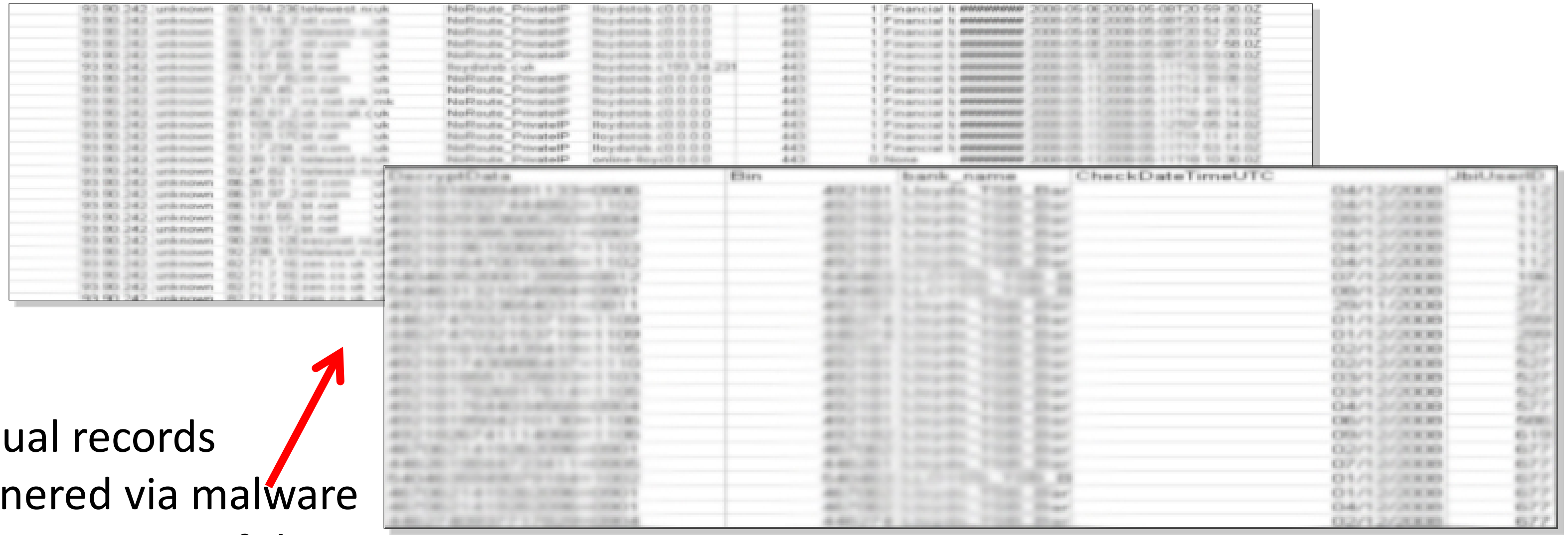
- Virtually all new mobile malware detected in Q2 2012 was directed at the Android platform,.



McAfee Threats Report: Second Quarter 2012, McAfee Labs, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf.

…where credentials can be purchased

- **2,800 customers at one bank identified in one month from one source within the Russian business network**



Actual records garnered via malware compromises of the Bank's customers

Bank's credit and debit card numbers being checked for status and available balance in preparation for fraud.

Souce "just buy it" Cchecker – Haxtor Network

Collaboration Strategies (U.S.)

- Cooperative Industry, Law Enforcement
  - FTC
  - National Institute of Standards and Technology (NIST)
  - FS – ISAC
  - Infra-Guard (FBI-Private Sector)
  - Identity Theft Assistance Center (ITAC) 41+ Members
  - Private Companies dedicated to ID Theft and Breach Issues
  - US Postal Inspection Service; US Secret Service; FBI
  - IRS and various Federal Law Enforcement work groups

- Shared Industry Information
  - Loss & Operational Metrics
  - VISA IRKI and Mastercard Loss Information
  - Early Warning Services
  - Hot files
  - International Fraud Prevention Programs (EW/BITS)
  - Shared Social Networks of Fraud
  - BITS, ABA, Financial Services Technology Consortium (FSTC)
  - Many Others

Collaboration Strategies (Canada)

- Cooperative Industry, Law Enforcement
  - Canadian Anti-Fraud Center (CAFC)
  - Competition Bureau
  - RCMP
  - Ontario Provincial Police Anti-Rackets
  - Canadian Identity Theft Support Centre (CITSC)
  - Private Companies dedicated to ID Theft and Breach Issues
  - Federal and Provincial Privacy and Data Protection Authorities
- Shared Industry Information
  - Loss & Operational Metrics
  - VISA IRKI and Mastercard Loss Information
  - Early Warning Services
  - Hot files
  - International Fraud Prevention Programs (EW/BITS)
  - Shared Social Networks of Fraud
  - BITS, ABA, Financial Services Technology Consortium (FSTC)
  - Many Others

SUMMARY OF (CANADIAN) REGULATORY ENVIRONMENT

Canada- Privacy Generally

- Broad (non-sector specific) Approach-
  - Federal
  - Provincial

- Common Risks and Environment compared to the U.S. with a different regulatory and cultural approaches

Canada- Privacy Generally

Federal

1. Privacy Act, R.S.C., 1985, c. P-21
   - *Public Sector*

2. Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 [a.k.a. PIPEDA]
   - *Private Sector*

– *No Federal health related data protection/privacy regulations*

Canada- Privacy Generally

Provincial

1. **Public Sector**- *Unique/Specific Regulations in each Province*

2. **Private Sector**- *Either*:
   a) PIPEDA applies (7 Provinces); or
   b) Provincial legislation that has been found to be substantially similar to PIPEDA applies. (3 Provinces)

3. ***Medical Data**
   a) 4 Provinces have laws governing the privacy of health related data
   - ***Alberta** [Health Information Act (HIA)]*
   - ***Manitoba** [Personal Health Information Act (PHIA)]*
   - ***Ontario** [Personal Health Information Protection Act (PHIPA)]*
   - ***Saskatchewan** (Health Information Protection Act (HIPA)]*

Canada- Privacy Generally

Federal-

- Office of the Privacy Commissioner of Canada

Provincial-

- Office of the Information and Privacy Commissioner
- Ombudsman
- Freedom of Information and Protection of Privacy Act Review Office
- The Commission d'accè s à l'information du Québec (the CAI)

Canada- Privacy Generally

Breach Notification Requirements-

1. **Provincial**-
   a) Alberta
      – PERSONAL INFORMATION PROTECTION AMENDMENT ACT, 2009
   b) Ontario (Health Data)
      – PERSONAL HEALTH INFORMATION PROTECTION ACT, 2004

2. ***Federal-**
   a) Office of the Privacy Commissioner of Canada (*Guidance NOT law*)
      – *KEY STEPS FOR ORGANIZATIONS IN RESPONDING TO PRIVACY BREACHES*

Canada- Privacy Generally

Breach Notification-

1. **Federal-**

- **BILL C-12-** An Act to amend the Personal Information Protection and Electronic Documents Act
  - **10.2** (1) Unless otherwise prohibited by law*, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control* if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

Self-Regulatory Security Requirements

Payment Card Industry Data Security Standards (PCI-DSS)

– Set of security requirements and standards promulgated by the payment card issuers (Visa, MasterCard, Discover, American Express, and JCB) regarding the storage and security of payment card related data.

Global Considerations

- Data Protection and Privacy need to be looked at as a global trade issue

- General Best Practices in Data Privacy from a Canadian Perspective is essentially a “Global” perspective.

- Sensitivity to global privacy considerations is necessary for risk managers of any companies with multinational interests

Privacy as a Right

The United Nations Universal Declaration of Human Rights, article 12, states:

- *“No one shall be subjected to arbitrary interference with his **privacy**, family, home or correspondence, nor to attacks upon his honor and reputation. **Everyone has the right to the protection of the law against such interference or attacks.**”*

Privacy as a Right

Article 8 of the European Convention on Human Rights:

- “***Article 8 – Right to respect for private and family life*** *…Everyone has the right to respect for his* ***private*** *and family life, his home and his correspondence…*”

Key Privacy Principles

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Key Principles for National Application):

- *Collection Limitation Principle*
- *Data Quality Principle*
- *Purpose Specification Principle*
- *Use Limitation Principle*
- *Security Safeguards Principle*
- *Openness Principle*
- *Accountability Principle*

Why GLOBAL Privacy considerations Matter

The importance of analyzing the regional differences in approaches to Data Protection and Privacy:

- Differences in categorization and treatment of data types in different regions

- Differing cultural views and treatment of Data Protection Privacy

BEST PRACTICES FOR EFFECTIVE

DATA RISK MANAGEMENT

Common Data Risk Consequences and Challenges

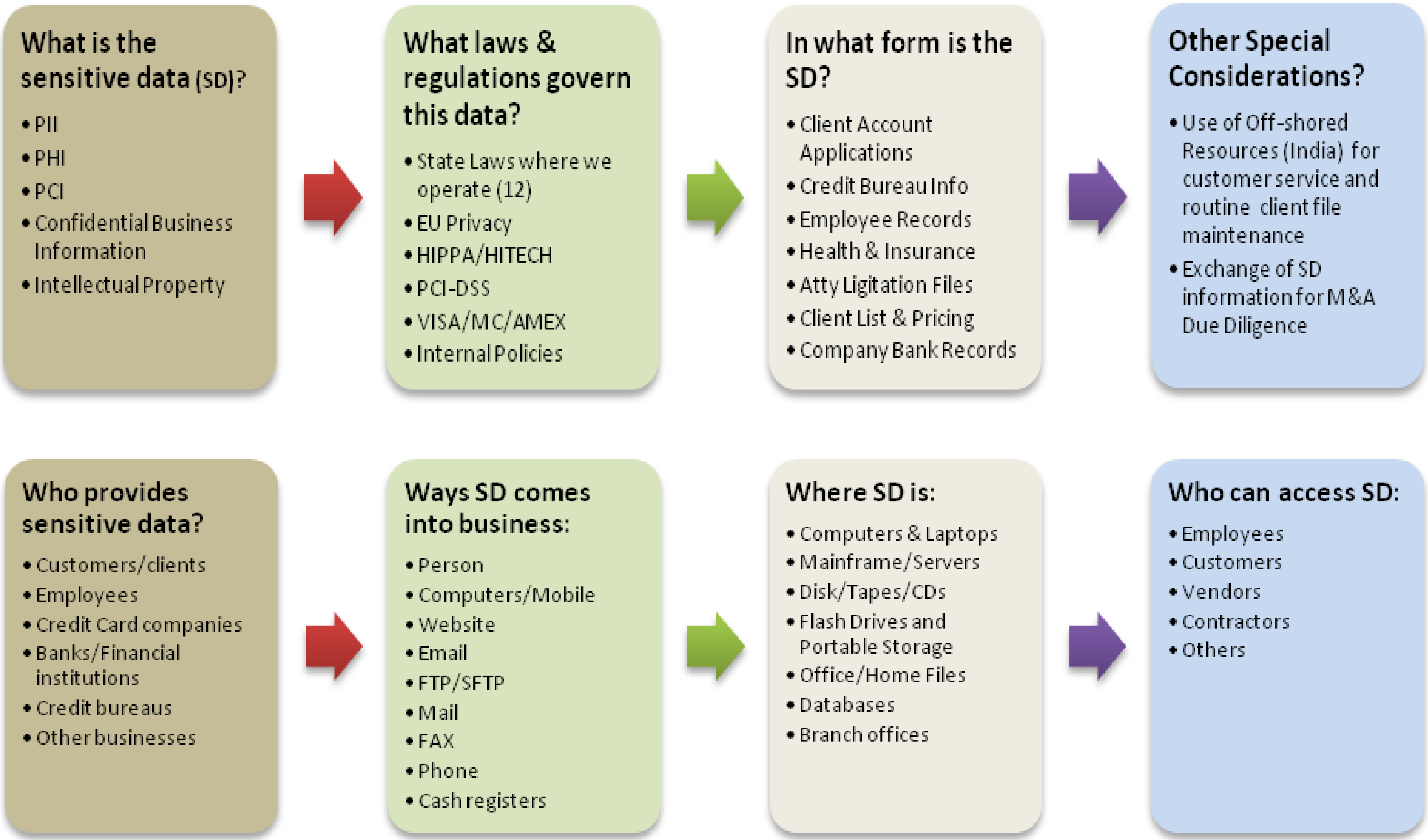
Consequences

- Disruption of service and damages
- Theft or exploitation of assets, information or resources

Challenges

- Likely significantly “underinvested” in data security based on current and emerging threats
- Potential state of denial in the executive suite
- Resource constrained
- Remediation can be costly and time-consuming
- Software development lifecycle is two-edged sword
- Countermeasures often defeated by the time they are deployed

Practical solutions for data risk management



What is the sensitive data (SD)?

- PII
- PHI
- PCI
- Confidential Business Information
- Intellectual Property

What laws & regulations govern this data?

- State Laws where we operate (12)
- EU Privacy
- HIPPA/HITECH
- PCI-DSS
- VISA/MC/AMEX
- Internal Policies

In what form is the SD?

- Client Account Applications
- Credit Bureau Info
- Employee Records
- Health & Insurance
- Atty Ligitation Files
- Client List & Pricing
- Company Bank Records

Other Special Considerations?

- Use of Off-shored Resources (India) for customer service and routine client file maintenance
- Exchange of SD information for M&A Due Diligence

Who provides sensitive data?

- Customers/clients
- Employees
- Credit Card companies
- Banks/Financial institutions
- Credit bureaus
- Other businesses

Ways SD comes into business:

- Person
- Computers/Mobile
- Website
- Email
- FTP/SFTP
- Mail
- FAX
- Phone
- Cash registers

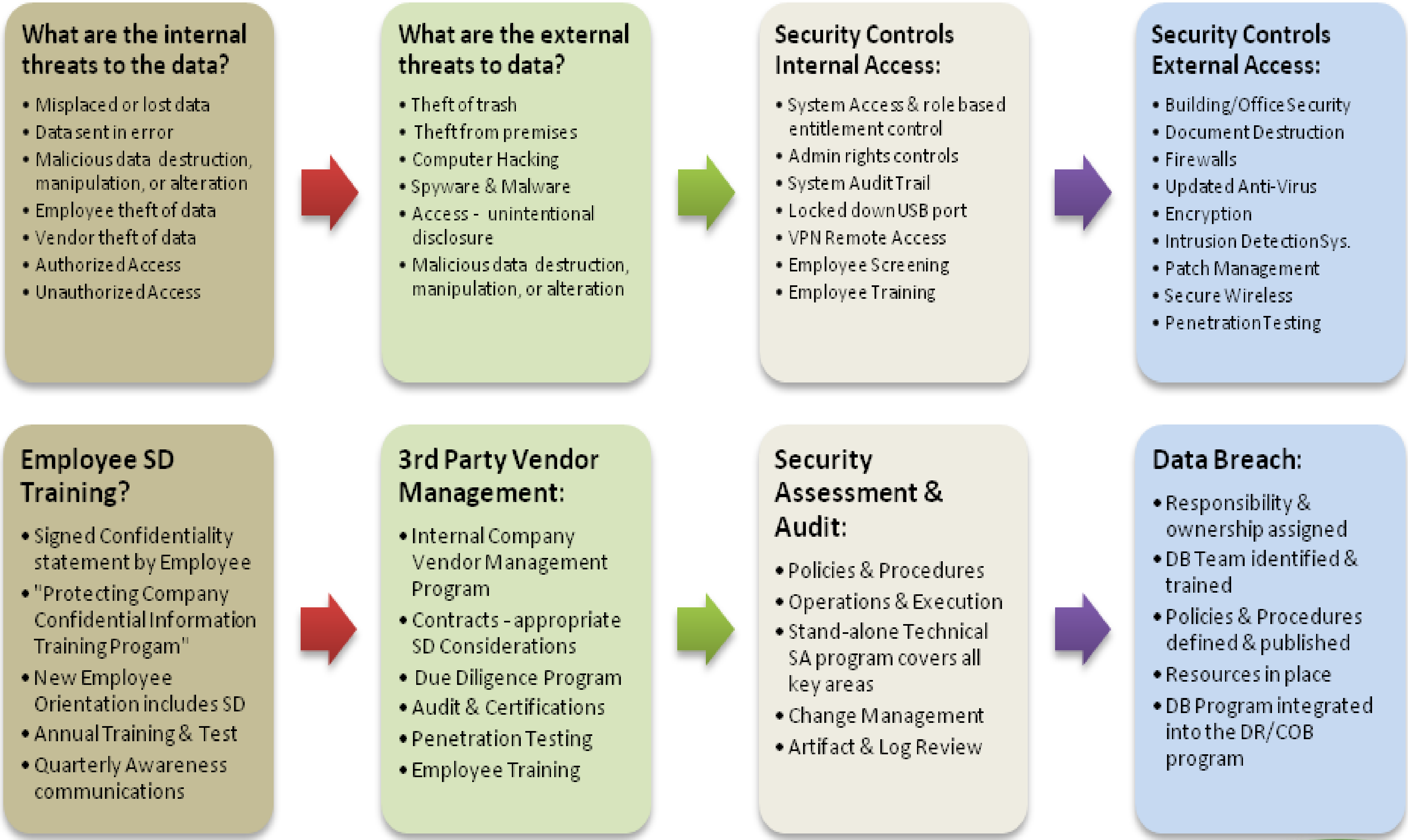
Where SD is:

- Computers & Laptops
- Mainframe/Servers
- Disk/Tapes/CDs
- Flash Drives and Portable Storage
- Office/Home Files
- Databases
- Branch offices

Who can access SD:

- Employees
- Customers
- Vendors
- Contractors
- Others

Practical solutions for data risk management



What are the internal threats to the data?

- Misplaced or lost data
- Data sent in error
- Malicious data destruction, manipulation, or alteration
- Employee theft of data
- Vendor theft of data
- Authorized Access
- Unauthorized Access

What are the external threats to data?

- Theft of trash
- Theft from premises
- Computer Hacking
- Spyware & Malware
- Access - unintentional disclosure
- Malicious data destruction, manipulation, or alteration

Security Controls Internal Access:

- System Access & role based entitlement control
- Admin rights controls
- System Audit Trail
- Locked down USB port
- VPN Remote Access
- Employee Screening
- Employee Training

Security Controls External Access:

- Building/Office Security
- Document Destruction
- Firewalls
- Updated Anti-Virus
- Encryption
- Intrusion Detection Sys.
- Patch Management
- Secure Wireless
- Penetration Testing

Employee SD Training?

- Signed Confidentiality statement by Employee
- "Protecting Company Confidential Information Training Progam"
- New Employee Orientation includes SD
- Annual Training & Test
- Quarterly Awareness communications

3rd Party Vendor Management:

- Internal Company Vendor Management Program
- Contracts - appropriate SD Considerations
- Due Diligence Program
- Audit & Certifications
- Penetration Testing
- Employee Training

Security Assessment & Audit:

- Policies & Procedures
- Operations & Execution
- Stand-alone Technical SA program covers all key areas
- Change Management
- Artifact & Log Review

Data Breach:

- Responsibility & ownership assigned
- DB Team identified & trained
- Policies & Procedures defined & published
- Resources in place
- DB Program integrated into the DR/COB program

Data Risk Assessments

- Expose vulnerabilities in organization
- Identify threats to organization
- Quantify potential adverse impact
- Document lack of controls
- Susceptible to misinterpretation

Data Risk Assessments

- Expose vulnerabilities in organization
- Identify threats to organization
- Quantify potential adverse impact
- Document lack of controls
- Susceptible to misinterpretation

- Want to do them
- Have to do them
- Should do them
- **Afraid to do them?**

Data Risk Assessments

- Expose vulnerabilities in organization
- Identify threats to organization
- Quantify potential adverse impact
- Document lack of controls
- Susceptible to misinterpretation

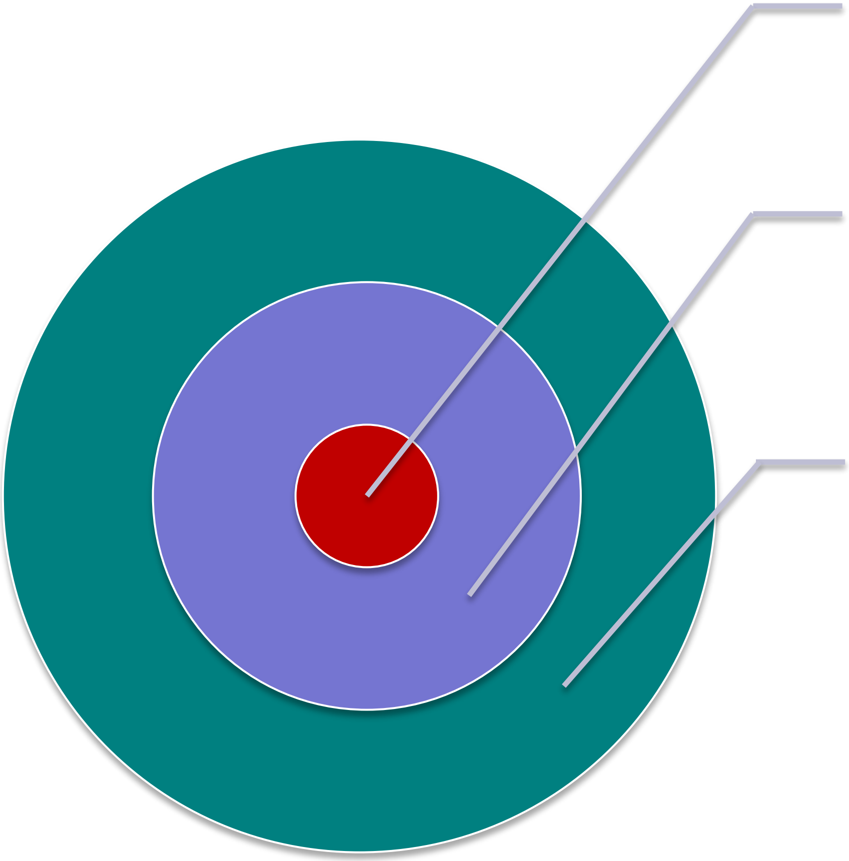
- Want to do them
- Have to do them
- Should do them
- **Afraid to do them?**

Solicitor Client Privilege

“Where legal advice of any kind is sought from a professional legal adviser in his capacity as such, the communications relating to that purpose, made in confidence by the client, are at his instance permanently protected from disclosure by himself or by the legal adviser, except the protection be waived.”

Evidence in Trials at Common Law, vol. 8 (McNaughton rev. 1961) at p. 543

Data Risk Assessments and Privilege:



To identify potential misinterpretations.

To form legal opinions regarding potential legal risks, exposures and responses.

To ensure that findings and conclusions will not form an admission of liability.

CONCLUSION

-OR-

A BETTER UNDERSTANDING OF WHERE TO GO FROM HERE

Immediate “To-Do” List to reduce risk/exposure

Defining the data and its collection:

- If the organization does not need it, do not collect it. *(Data is not an asset, it can be toxic.)*

- If data must be collected, collect only what is needed.

Immediate “To-Do” List to reduce risk/exposure

Defining the data and its collection:

- If data is needed, control it and encrypt it.
- When data is no longer needed, get rid of it – securely.

Immediate “To-Do” List to assess & cover risk

- Complete high level “data” audit to determine
  - Type of personal information you retain
  - What provinces/states/countries do your customers/employees live in?
- Complete a Security audit to determine weaknesses

Practical solutions for data risk management
Immediate “To-Do” List to assess & cover risk

- Determine if you have adequate insurance coverage for your risk:
    - 1st Party Costs (consults, mailing/notice, call handling, forensics, etc.)
    - 3rd Party Costs (Regulatory or Civil Liability and defense)

Practical solutions for data risk management
Creating Documentation and Programs

- Written Information Security Program
- Breach Response Plan
- Business Continuity Plan
- Data/Document Retention and Destruction Plan
- Data Security and Privacy Awareness Program

General Best Practices in Data Privacy (From a Global Perspective)

Figure out the applicable entity’s “data Footprint”

- What type of data is collected?
- From Whom?
- From where?
- For what Purpose?
- Who can access that Data?
- Where is data being stored, processed, etc. ?

General Best Practices in Data Privacy (From a Global Perspective)

Examine regional, national, state, provincial and even municipal privacy requirements:

- Is your industry regulated?
- Is privacy in the applicable jurisdiction regulated?

General Best Practices in Data Privacy (From a Global Perspective)

Develop a “privacy framework” within your data risk management regime that reflects your business from a:

- philosophical standpoint;
- business standpoint; and
- operational standpoint

General Best Practices in Data Privacy
Integrate a Privacy-by-Design (PbD) Approach:

1. Proactive not Reactive;
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality -Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

Questions?

Eduard Goodman, J.D., LL.M., CIPP-US/C

EGoodman@idt911.com

480-355-4940

IDentityTheft 911®
Protecting identities. Enhancing reputations.

Enjoy the rest of the 2012 RIMS Canada Conference!