

# **Looking in the Mirror: How Do We Secure Our Firms From Ourselves**

**Ivaylo Nikolov - Davies Ward Phillips & Vineberg LLP**

**Venky Srinivasan - Stikeman Elliott LLP**

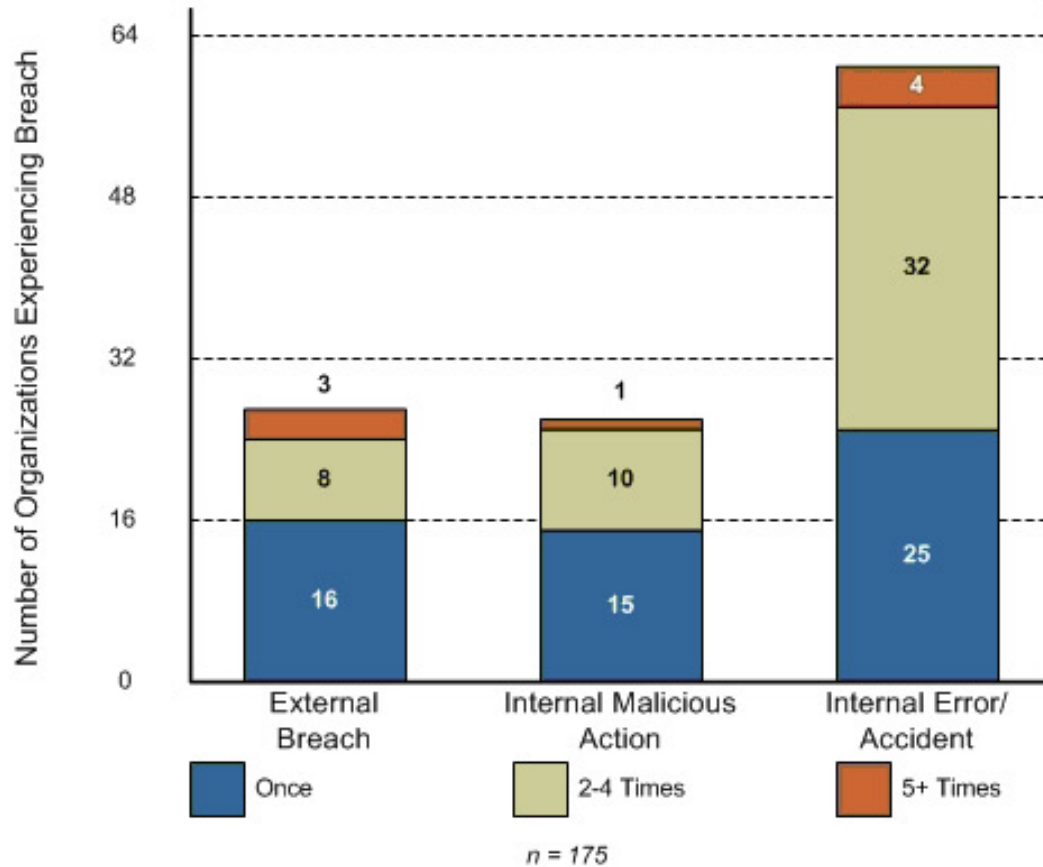
**John Esvelt - Fraser Milner Casgrain LLP**

**Jim Soenksen - Pivot Group**

## Separating Fact from Fiction

- Recent Info-Tech study shows that a significant number of companies experienced security breaches
- Security breaches are classified into three types – externally sourced, internally sourced: employee error and internally sourced: malicious activity
- Internally sourced breaches outnumber external breaches by a factor of 3:1
- Perimeter protection is only part of the solution
- While firms spend significant resources to protect themselves from external threats, insiders cause significantly more security breaches

## Security Breaches by Type



# Data Privacy Legislation; Client Demands & Expectations

In addition to our clients' high expectations and demands, data privacy is called for in governance frameworks such as COBIT and ISO 17799, but is also a requirement of several privacy and fraud-related laws:

- Sarbanes-Oxley (publicly traded companies)
- FISMA (federal government and government contractors)
- Basel II (international banks)
- PCI DSS (merchants and credit card service providers)
- GLBA (banks and financial services institutions)
- HIPAA (healthcare providers and payment plans)

# Data Privacy and IT Personnel: Policies and Responsibilities

**Create and/or amend policies and job descriptions.** Policy must drive and direct IT worker roles, responsibilities, and obligations as they relate to data privacy. Create and maintain the following relevant policy documents such as:

Non-disclosure and non-competition forms (to protect sensitive data, corporate assets, trade secrets, etc.).

Systems administrator code of conduct (for establishing a professional code of ethics for IT staff using sensitive data).

Account privileges and expiry policy (for closing old network IDs, e-mail accounts, etc.).

Employee manual (encompassing technology acceptable use policies).

**Separate responsibilities.** This will reduce the opportunities for unauthorized or unintentional modification or misuse of the organization's assets, by employing a three-pronged approach:

1. Segregation of duties.
2. Least privilege.
3. Identity management.

## Data Privacy and IT Personnel: Segregation of Duties I

**Segregation of duties** is conducted for the purposes of determining who has access to the enterprise's systems and processes, and where potential conflicts may exist. Conflicts arise when an employee's job responsibilities overlap into another area, possibly allowing financial fraud to occur. Ensuring proper segregation of duties minimizes these conflicts, enhances data privacy, and creates compliance with Section 404 of Sarbanes-Oxley.

- Segregation of duties is considered a type of internal control. Failure to adequately demonstrate the effectiveness of internal controls could lead to a negative audit outcome. In the case of non-traded companies (i.e. those that aren't governed by SarbOx), duty segregation should be viewed as a best practice that will improve security and help eliminate conditions wherein employee fraud could transpire.
- Segregation of duties can also be used for IT departments at an operational level to improve error rates and increase reliability. For example, an application development team may have its duties segregated so that code writing, testing, and deployment are each conducted separately by three individuals, thus helping to ensure code integrity.

# Data Privacy and IT Personnel: Segregation of duties II

Table 1. Sample Segregation of Duties Matrix

	Control Group	Systems Analyst	Application Programmer	Helpdesk Manager	End User	Data Entry
Control Group		X	X	X		X
Systems Analyst	X			X	X	
Application Programmer	X			X	X	X
Helpdesk Manager	X	X	X		X	X
End User		X	X	X		
Data Entry	X		X	X		

X = Combining these roles may create a privacy conflict and control weakness.

## Data Privacy and IT Personnel: Least Privilege

**Least privilege** is not a requirement but is considered a security best practice. Least privilege is a principle of security in which IT staff is granted the absolute minimal level of access rights required to complete their duties. Least privilege requires the mapping of access rights to business requirements.

- Intermittent elevation of access rights for IT workers will sometimes be required for a certain project. Still other IT staff will require full access to their machines' capabilities. Applying least-privilege principles to access policies in general will allow IT to customize security mechanisms according to business needs.
- On the vendor side, Microsoft is currently promoting its Least-Privileged User Account (LUA) concept, which is supported by the Vista operating system. The LUA construct acknowledges that new user accounts are set to "Administrator" as the default setting in Windows installations. LUA removes this danger by resetting user accounts to limited access configurations.

## Data Privacy and IT Personnel: Identity Management

- **Identity (ID) management** is a technology component that will be needed to help enforce, automate, and log user activities as they relate to data access and privacy. Identity management is a broad term meaning a system or solution that identifies individuals within the network, and then controls their access to network resources by associating user rights and restrictions with the established identity.
  - ID management software typically encompasses a combination of password synchronization/reset/recovery, single sign-on, digital certificates, tokens, and policy-based access management software.
  - The main value of ID management is that it eliminates manual user provisioning and access rights processes. In order to achieve this value, focus efforts on automatic process facilitation based on business, IT, and user needs
  - ID management also brings new efficiencies such as fewer calls to the help desk, shorter call resolution time lapses, faster authorization and signoff, and so on.
  - ID management vendors include Computer Associates, Courion, HP, IBM, Novell, and RSA Security.

# Data Privacy and IT Personnel: Incident Response Program

Experience shows that most organizations don't think about how to respond to a computer security incident until after they have experienced a significant one! This problem is common; many organizations have not assessed the business risk of having no formal incident-detection and response mechanisms in place.

Be Prepared

Policies

Procedures

Incident Response Team

## Private Data Protection

### Checklist for Monitoring Where PII or Personal Information is Stored

PII OR PERSONAL INFORMATION TYPE IN COMBINATION WITH FIRST NAME OR FIRST INITIAL AND LAST NAME	ENCRYPTION		LOCATION								
	ENCRYPTED	ENCRYPTION KEY NOT WITH DATA	DO NOT COLLECT	NETWORK	LAPTOP	USB DRIVE	E-MAIL	BLACKBERRY OR PDA	CELL PHONE	COMPUTER HARD DRIVE	CD OR DVD
Address and telephone number (by itself it is not considered a breach because of its availability in public records)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Driver's license or state personal identification card number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Social Security Number (SSN)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Place of employment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Employee identification number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Employer or taxpayer identification number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Government passport number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Health insurance identification number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mother's maiden name	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Demand deposit account number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Savings account number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Financial transaction device account number or the individual's account password	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Stock or other security certificate or account number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit card account number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vital record	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Medical records or information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Demand deposit or other financial account number, or credit card or debit card number in conjunction with any required security code, access code, or password that would permit access to any of the individual's financial accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>