Information Security Awareness Training

Version 2.12, June 2015

Sonata Internal

- Information Security Management Group

Agenda

- What is Information Security
- Information Security – Three Dimensions of Information Security
- The need for Information Security at Sonata
- Security Incidents and Breaches around the world
- Protecting Information Assets
- HR Security
- Physical and Environment Security
- Guidelines to be followed at Workplace
- Data privacy and confidentiality
- Password policy
- Security Incidents
- Business Continuity and Disaster recovery

What is Information Security?

Information Security – What does it Mean?

CIA TRIAD – Three Dimensions of Information Security

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Confidentiality

Integrity

The property of safeguarding the accuracy and completeness of assets

Availability

Asset is accessible and usable upon demand by an authorized entity

The Need for Information Security at Sonata

- Protect confidentiality and integrity of customer data
- Protect confidentiality and integrity of data of Sonata and its employees
- Protect company assets and people
- Compliance to Internationally Recognized Standards like ISO 27001, ISO 20000, etc.
- Improved Adherence to Local and International Laws and Regulations like IT ACT 2000, PCI DSS, FDA, DPA, SOX , HIPPA etc.
- Risk Management
- Better Brand Image
- More Business

Some Security Incidents and Breaches around the World

□ “Retailer TJX reports massive data breach: The TJX Companies, a large retailer that operates over 2,000 retails stores suffered a massive computer breach on a portion of its network that handles credit card, debit card, check, and merchandise transactions in the U.S. and abroad. Hackers had access to their network for about two years”

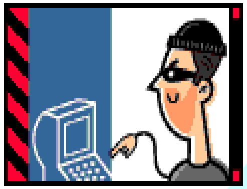
HSBC Bank fined £3.2 million by FSA for losing details of 180,000 life insurance customers – unencrypted disk lost in the post

Bank of New York Mellon suffers physical security breach – potential compromise of personal details of 12.5 million customers – lost data back up tape

Heartland Payment Systems hacked: tens of millions of transactions compromised – computers infected with malware

Some Security Incidents and Breaches around the World (Cont'd)

- Boston-based cryptography firm RSA suffered a massive network intrusion that resulted in the theft of information related to its SecurID tokens. Forty million people use the tokens to access the internal computer networks of 25,000 corporations, government organizations and financial institutions.



Hackers penetrated the internal networks of Epsilon , a Texas-based firm that handles email communications for more than 2,500 clients worldwide. The companies affected by the Epsilon hack included Ameriprise Financial, BestBuy, Capital One Bank, Citi, JPMorgan Chase, TiVo, U.S. Bank and dozens more.

One group stole the personal information of 102 million registered users of the PlayStation Network (PSN) and other online gaming services.

NASA's Goddard Space Flight Center, lost confidential satellite data in an April hack, and InfraGard, an FBI affiliate that was compromised by the hacking group LulzSec, which also attacked PBS, Nintendo and Fox.

Protecting Information Assets

Inventory and classification of information assets

Example of assets at Sonata

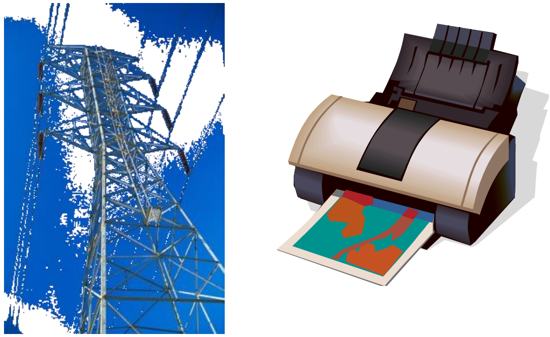
Electronic Assets

Core IT Equipments

Software

Paper Assets

People



Support / Service Equipments

Protecting Information Asset (Cont'd)

Information assets require adequate protection:

Responsibility For Assets

- *Perform inventory of assets in your team/project*
- *Set ownership for your assets*
- *Follow policy for acceptable use of assets*

Information Classification

- *Follow classification guidelines*
- *Follow information labelling and handling guidelines*
- *Prepare Document Distribution List (DDL),*

It is an indicator to the receiver of information:

- *About sensitivity of the information*
- *With whom can this be SHARED with*
- *About how to handle (store, transmit, delete/ destroy) the information*

Human Resources Security

Informing employees of their security obligations prior to, during and after employment

Prior to Employment

- *Facilitate for proper screening before engaging*
- *Observe confidentiality clauses*
- *Make sure all terms and conditions of employment are clearly understood and accepted*

During Employment

- *Understand the specified roles and responsibilities assigned to you, be it an employee, contractor, or a third party*
- *Attend information security awareness, education, and training as and when conducted*
- *Make sure you and your colleagues always follow sonata security policy*

Termination or Change of Employment

- *Return all the assets that have been provided*
- *Make sure all your access rights are disabled*

Physical and Environment Security

Ensuring Security at Workplace

Piggybacking is not allowed !

Use Your Own Access Card !!!

- *Do not tailgate*
- *Do not allow tailgating*
- *Do not give access without authorization*

… And Outside Workplace

Physical and Environment Security (Cont'd)

Physical protection of computer facilities, telecom equipments including servers, desktops and laptops.

No Photography within the premises of Sonata office (even with a camera mobile)

Visitor Management

- *Non business visitor should be entertained at reception only*
- *Business visitors should be allowed to enter areas based on requirement and after proper approval*
- *Visitors have to be escorted at all times*
- *Visitors should visibly wear the visitor badge all the time*

Guidelines To Be Followed At Workplace

Email / Internet Usage

- *Align to Acceptable Usage Policy, follow email/ Internet Usage policy (no spam mails, no objectionable content/images)*
- *Do not use Internet to listen online music or other personal gain (stock trading, e-business, chain marketing etc)*

System Security

- *Do not disable or change system wide settings related to event logging, Antivirus, firewalls, VPN and Operating System.*
- *Do not download any kind of software or exe file from Internet. If required, raise a Job Card, get proper approval and let the IT Infrastructure team download and install it.*

Media Usage

- *Avoid direct disk sharing with Anonymous access*
- *Ensure that all CDs & media entering Sonata premises are declared at entry point / reception*
- *Always scan media from an unknown source for virus before using*

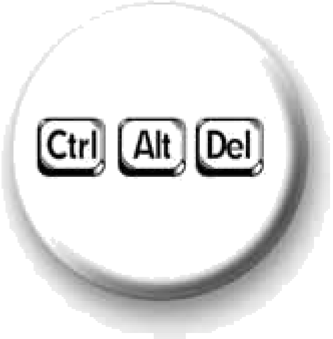
Guidelines To Be Followed At Workplace (Cont'd)

Information Backup

- *Plan data backup based on criticality*
- *Ensure restoration checks for all backups, and offsite storage*

Copyright Compliance

- *Do not replicate copyrighted materials*
- *This includes copying music files onto PCs*



Software Licensing Compliance

- *Use licensed software diligently, do not abuse licenses*
- *Use freeware, trial ware, shareware only after authorized approval*
- *Software that are free for "personal use" cannot be used for any activity in Sonata*
- *Evaluation software - to be used for evaluation purpose only*

Protect your workspace

- *Lock terminal when away*
- *Ensure clear desk and clear screen policy*
- *Ensure that screen savers are enabled to start at 3 minutes of inactivity*

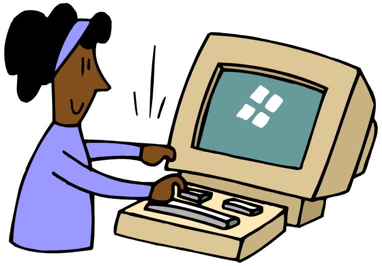
Data Privacy and Confidentiality

Data Privacy

- *Sonata has rolled out a new policy for Data Privacy Last year (2014)*
- *All employees, contractors, consultants, third party data processors and all those with access to personal data on behalf of Sonata are responsible for complying with the Sonata's Data Protection Policy & Procedures.*
- ***Data Privacy policy deals with***
  - *The Collection and use of personal data*
  - *Sharing the Personal Data*
  - *Security of Personal Data*
  - *Physical Security of Personal Data:*
  - *Electronically held Personal Data:*
  - *Sending Personal Data via Email:*
  - *Access to Records containing Personal Data:*
  - *Retention and disposal of personal data*

Data Privacy and Confidentiality

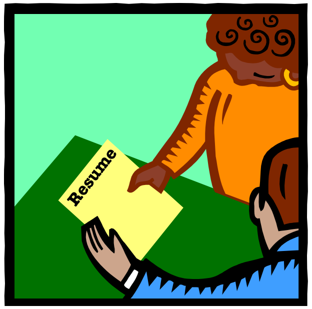
- *Treat customer data, including their customer's and even the test data as confidential. Access to it should be with specific permission, even for testing purpose.*
- *Refrain from moving, copying or emailing the customer data, source code or any another data from a control area to another share outside the ODC or Sonata.*
- *Do not email, upload or copy any part of source code or customer data or test data to any online storage, public discussion forum or websites.*
- *Ensure that the Control Area/SCM tool has Restricted Access Control and is reviewed regularly.*



- *Refrain from using the customer name in your personal CV, online portals or professional networking sites like LinkedIn, etc.*

Customer Network Access

- *While on customer network or connected to it, do not access illegal websites or do not perform any activity against customer policy.*
- *When team member is released from the account, make sure that his/her login ids to customer network is disabled.*



Data Privacy and Confidentiality (Cont'd)

Do not share Sonata issued assets with anybody, even with your close friends or relatives

Use Shredders for disposal of confidential papers and CDs. Do not just throw away!

Password Policy

- *Do not use a password which is easy to guess*
- *Never share your password with others*
- *Passwords should be a minimum of eight (8) characters*
- *Without leading or trailing blanks*
- *Passwords should contain both alphabetic and non-alphabetic characters. It should contain upper, lower case characters and numerals*
- *Passwords should be changed at least once in every 45 days*
- *All passwords should be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties*

✓ Use Job Card to raise requests for any changes, issues in IT infrastructure.

Password Strength

Pattern	Calculation	Result	Time to Guess ($2.6x10^{18}$/month)
Personal Info: interests, relatives		20	Manual 5 minutes
Social Engineering		1	Manual 2 minutes
American Dictionary		80,000	< 1 second
4 chars: lower case alpha	26^{4}	$5x10^{5}$	
8 chars: lower case alpha	26^{8}	$2x10^{11}$	
8 chars: alpha	52^{8}	$5x10^{13}$	
8 chars: alphanumeric	62^{8}	$2x10^{14}$	3.4 min.
8 chars alphanumeric +10	72^{8}	$7x10^{14}$	12 min.
8 chars: all keyboard	95^{8}	$7x10^{15}$	2 hours
12 chars: alphanumeric	62^{12}	$3x10^{21}$	96 years
12 chars: alphanumeric + 10	72^{12}	$2x10^{22}$	500 years
12 chars: all keyboard	95^{12}	$5x10^{23}$	
16 chars: alphanumeric	62^{16}	$5x10^{28}$	

Security Incidents

Identifying and Reporting Security Incidents in Sonata

- *Do you think that security norms are not adhered to in your project work?*
- *Do you see others who do not comply to the norms stated?*
- *Do you see some things which could lead to failure of security?*
- *Do not ignore or turn a blind eye towards any security incident!*

Some instances of security incident:

- *Copying/moving data out without authorization*
- *Moving company assets without authorization*
- *Password sharing*
- *Abuse of company resources*
- *Unauthorized access, etc.*

Report such incidents to the Information Security Manager or to a Senior Manager:

- *Immediately without any hesitation*
- *Even if you are unsure of trueness of the incident*

Business Continuity and Disaster Recovery

Protecting, maintaining and recovering business-critical processes and systems

- *Implement and follow the risk assessment as per guideline*
- *Develop and implement continuity plans including information security*
- *Test, maintain and re-assess your business continuity plans*

Convenience vs. Security

We cannot carry out normal functions or timely delivery, if we follow the mentioned processes!

- Work cannot stop. When a team member is not available, need to share the password

  Issues

  - *Remember, it could be misused and you will be held responsible*

  Right way

  - *Share data / folders, NOT password*
  - *Identify backups for key positions*
  - *Plan ahead*

- I need to install a software/freeware right now so as to meet the project deadline

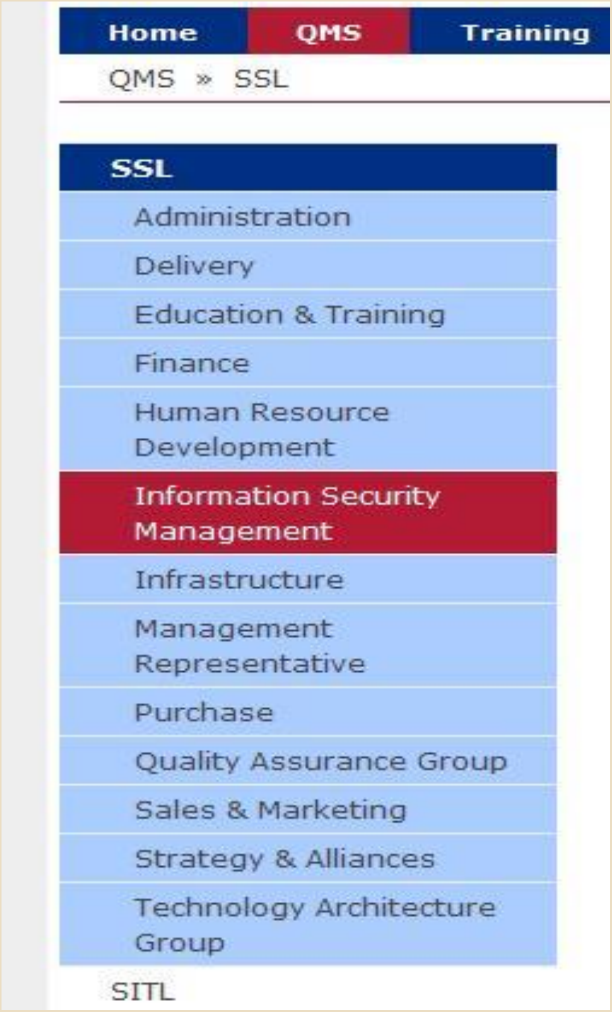
  Issues

  - *Company will face a legal action, if software is used without license or violating the its agreements*
  - *A software from an un-trusted source may contains a virus, your PC and the entire network will get infected*

  Right way

  - *You need to go through the **support** and proper approval process which helps understand the associated risk (technology / legal)*

Info Sec related links



To access Sonata Security Policy, Procedures and Guidelines, visit ‘Information Security Management’ section in the QMS (Quality Management System) Intranet site:

QMS -> SSL -> Information Security Management

Incident reporting: ‘Security Connect’

Sambandh -> Quick Links -> Security Connect

Contact us:

Security.incident@sonata-software.com

Quiz Time

1. Which one is the best password combination to be used in Sonata?

- password
- August2010
- Kumar1984
- 4uM@r!27 ✓
- Sonata123

2. In case of an emergency or crisis what is the order of preference for safety?

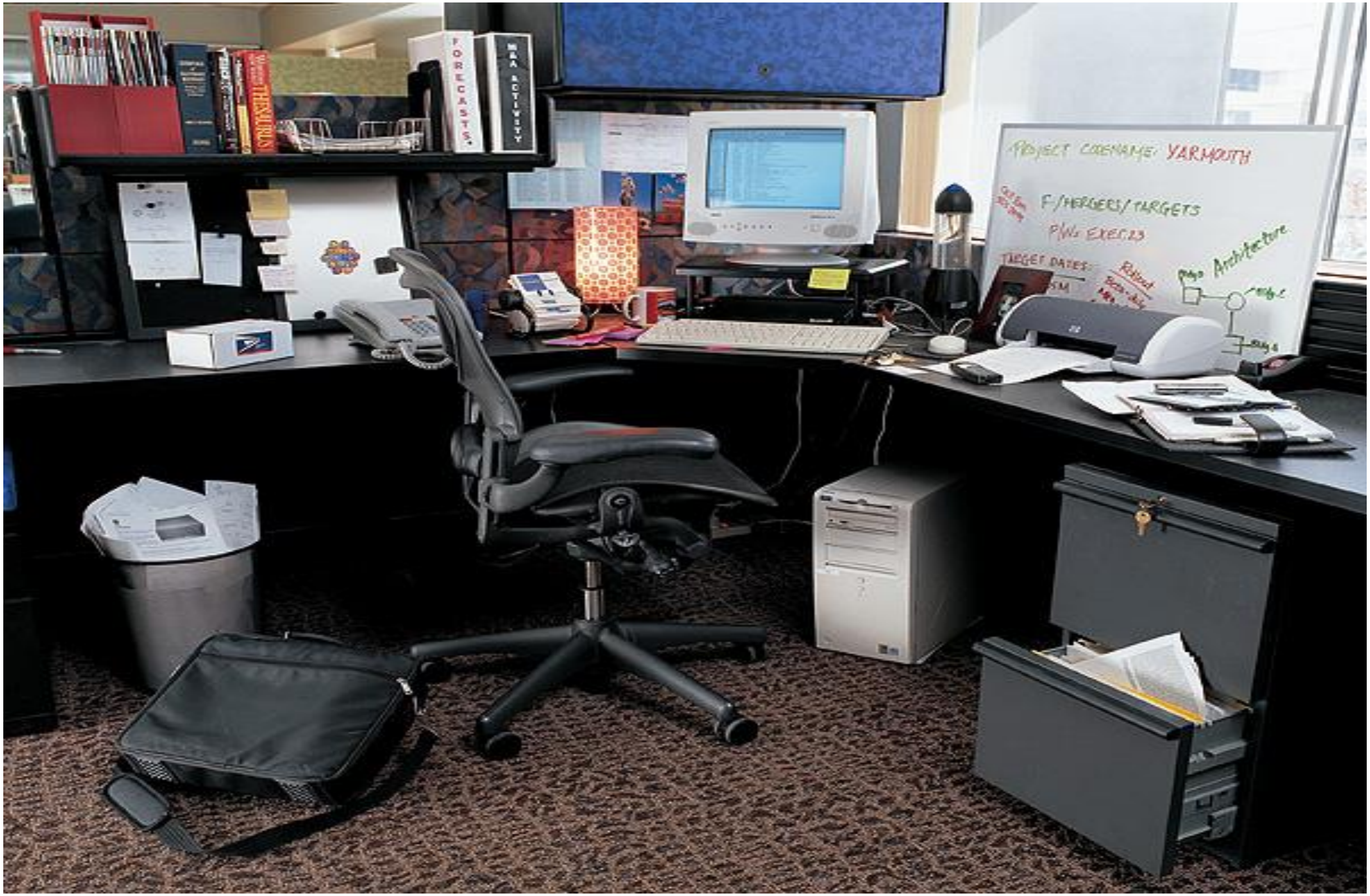
- Building, computer equipment, data (backups, etc), People
- Data (backups, etc), People, computer equipment, Building
- People, data (backups, etc), Building, computer equipment ✓
- Computer equipment, Building, People, data (backups, etc)

Quiz Time

- 3. I have been assigned important work and I have emailed them to my personal id so that I can continue to work at home.
  - It is ok as long as you don't leak the data yourself.
  - It is ok if your PL agrees.
  - My home computer is as secure as work computer hence it is safe.
  - [✓ It’s a violation of Information security policy of Sonata and the client.]
- 4. What is considered as an asset?
  - Information- Files, documents, contracts
  - Software - Applications, Utilities
  - Hardware – Laptops, PCs, servers
  - [✓ All of the above]
  - None of the above

Link to Information Security Quiz: https://ismsquiz.sonata-software.com

What's Wrong with This Picture?



Sonata Security Vision

"To protect the confidentiality, integrity and privacy of data and information belonging to Sonata, it's customers, employees and business associates and to achieve this by implementing industry standards and best practices"

Q & A

“The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards”

“Security is similar to a chain, its total strength is equal to its strength at the weakest position”

SONATA SOFTWARE

Thank You