KREATIO
MONETIZING CONTENT

Information Security Awareness Program

Information Security Awareness Program

Prepared for:

All Associates of Kreatio

Prepared by:

Information Security Team of Kreatio

This presentation is confidential and is solely for the purpose of sharing information. No part of it may be circulated, quoted, or reproduced for distribution without prior written approval from Kreatio.

Synopsis

- What is Information and Where It Can Be Found?
- What Is Information Security?
- Understanding Information Security and Importance Of CIA
- Information Security Mission Of Kreatio
- Information Security Mission & Objectives Of Kreatio
- Data Classification Standard Of Kreatio
- Certifications Of Kreatio
- Impacts Of Information Security Breach
- Important Data Breaches of 2015 & 2016
- Security Do’s and Don'ts
- Security Incidents and Procedure of Reporting
- More Details - Policies and Procedures
- Kreatio Global Information Security Organization

What is information and where do we find it?

"**Information** is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected"

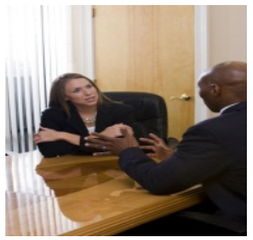
Printed or written on paper

Stored electronically

Transmitted by post or using electronic means

Shown on corporate videos

Verbal - spoken in conversation



"…….Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected"

What is Information Security?

The process of ensuring information, business systems and information assets are protected, secure and available to achieve C-I-A.

Understanding Information Security: CIA

Confidentiality: *Ensuring that information is accessible only to those who have authorized access*

Integrity*: Safeguarding the accuracy and completeness of information and processing methods*

Availability*: Ensuring that authorized users have access to information and associated assets when required*

Information Security Mission Of Kreatio

To Protect Customer, Company And Employee Information Assets

From All Internal And External Threats.

Kreatio Security Objectives

- To protect all Information against unauthorized access
- To ensure Confidentiality of Information
- To maintain Integrity of Information
- To comply with all Regulatory and Legislative requirements

- To prepare, maintain and test Business Continuity Plans
- To provide Information Security Trainings to all users
- To report, investigate and rigorously prosecute any breach of Information Security actual or suspected

Data Classification Standard of Kreatio

Kreatio classifies its information into four types :

Restricted – Information that is extremely sensitive and of highest value to Kreatio and is intended for use only by named individuals within the company. Such information assets have the potential to have a negative financial, competitive or legal impact. The number of people provided access to this information is very limited.
Eg., Information on financial forecasting; Kreatio strategic information; Earnings estimates; Major litigation information; System or application Passwords; Data File Encryption Keys; Marketing Strategy, etc

Confidential – Information that is sensitive within the company and is intended for use only by specified groups of employees. Access is granted based on business justification and approval.
Eg., Departmental memos; Client lists and contact information ; Social security numbers, home addresses and telephone numbers ;Health information; Benefits, employee earnings, payroll data

Internal - Non-sensitive information available for internal release. Such information is the property of Kreatio and Kreatio has the sole right over this information. This form of information must be used within Kreatio and not shared externally or with third parties.
Eg.,Project plans ; company news letters; *Organization charts ; Employee contact information ; Internal meeting presentation materials*

Public - Non-sensitive information available for external release.
Eg., Job vacancies ; Published press releases ; *information available on www.Kreatio.com*

Impacts Of Information Security Breach

- Customer Related Information
- Employee Information
- Kreatio “Internal”
- Legal and Regulatory compliance
- Physical security
- Logical security

Important Data Breaches of 2015 - 2016

- In August 2015, 200,000 users of WhatsApp's web-based service were hit in a cyber attack that let hackers compromise personal data using just their phone number. Hackers sent vCard's to random phone numbers. The vCard sent by the hackers contained a malicious code that would distribute bots, ransomware and remote access tools (RATs) on a person's phone or PC. Bots can slow down a person's system, ransomware makes people pay money to regain access to their own data, while RATs allows hackers to remotely access a device.

- In November 2015, hackers have found a new way to hack Android Smartphone and remotely gain total control of it, even if the device is running the most up-to-date version of the Android operating system. Security researchers discovered a critical zero-day exploit in the latest version of Chrome for Android that allows an attacker to gain full administrative access to the victim's phone and works it on every version of Android OS. The exploit leverages a vulnerability in JavaScript v8 engine, which comes pre-installed on almost all (Millions) modern and updated Android phones. All the attacker needs to do is tricking a victim to visit a website that contains malicious exploit code from Chrome browser. Once the victim accessed the site, the vulnerability in Chrome is exploited to install any malware application without user interaction, allowing hackers to gain remotely full control of the victim’s phone.

- UK-based telecom client TalkTalk has suffered a major cyber attack in October 2015 that has compromised the personal and financial details, including bank account information, of some 1,57,000 customers. Three Wipro employees in Kolkata have been arrested in connection with a security breach in the customer records . This brings negative publicity to Wipro along with legal repercussions and loss of business.

- Infosys's BPO operations has suffered a similar situation when several Infosys junior and mid-level employees were caught in the overbilling of Apple, a major Infosys client. It led to the exit of the CEO and CFO of the BPO operations.

- Britain's HSBC, which is one of the world's largest banks, warned its customers on January 29’ 2016 that it's been targeted by distributed Denial- Of-Service Attacks that continue to disrupt customers' access to online banking services .

Physical Security – Do's

- Wear photo ID badge and ensure visibility while in the building.

- Swipe your access card when entering/exiting the building.
- Visitors must sign in at reception and must be escorted at all the times.
- Lock office doors, cabinets and drawers when unattended or when you are not in vicinity.
- Ensure the security of laptops at all times while in the office, car and at home.
- Sensitive documents being printed should be cleared off printers immediately

Physical Security – Do's

- Personal belongings should be left at the security or in the lockers assigned.

- Throw confidential reports in the trash by shredding them first. It can protect you from identity theft

- Paper and computer media should be stored in secured place under lock and key when not in use

Physical Security - DON'Ts

Access Card Accountability

- Do not loan access cards
- Do not swipe for others

Asset Movement

- Do not carry any business assets outside the premises without prior approval
- All materials should go out only with the gate pass approved by an authorized signatory.
- Avoid bringing any personal assets to the workplace

Physical Security - DON'Ts

- **Photographic Equipments in Operation floors are not allowed**

- **Personal Belongings like Bags are not permitted inside the following areas:**
  - Operations/Production areas
  - Server Room
  - UPS and DG Area

Logical Security

Password Security – Do's and Don'ts

- Do NOT have the User Name the SAME as the Password
- Mix upper and lower case and have alphanumeric Passwords
- Do NOT share Passwords across Systems or Applications
- Do NOT Write it Down Anywhere as it can be Easily Found
- Change Passwords Frequently – At Least every 45 Days
- Do NOT Disclose Passwords – NOT even to System Administrators.

Logical Security - Do’s and Don'ts

- **Email Usage**
  - Use Email only for Business Purposes.
  - Do Not Open Attachments from Unknown Sender
  - Do Not Forward Chain Mails
  - Don’t Click on Reply All – always
  - Never Send Any Critical Information via Emails, Instant Messenger or Other Modes.

- **Internet Usages**
  - Browse Only Business Specific Sites
  - Browsing Non-Business Websites Are Prohibited (refer to AUP)
  - Exceptions Are Addressed Based On Business Justification And Client’s Approval

Leaving your System???

- Log off or Lock your workstation when you are away from desk or cubicle.
  - Press CLT+ALT+DEL and select ‘Lock Computer’ or Log Off
  - OR Press + L

Security Incidents and Procedure Of Reporting

What is a security incident?

- Any event that compromises CIA of information.

- Event could be Customer, Physical, Logical, IT related, Policy related etc.

- Sometimes a security weakness precedes an incident

Some examples are:

Theft

Physical security access control failure

Misuse/tampering with information

Virus outbreak

Violence or Riots

Unauthorized physical access

Unauthorized distribution of information

Hacking etc.

Process for Reporting Security Incidents

- You need to play your role
  - Report all security incidents to your supervisor and to the Information Security Team **complaints@kreatio.com**
  - The incident management committee will investigate and take appropriate disciplinary action
  - The template for Incident Report can be obtained from the **https://edms.kreatio.com/select/documents**

Incident reporting is Every one's Responsibility

REMEMBER –

Be Compliant, Be Alert and Watchful, Take Onus For The Security of Your Own Organization....

Information Security Begins With You

Thank You