Information Security

Last Updated: 14-Sep-2014

June 6, 2014 Miami-Dade County,Florida

The county of Miami-Dade informed employees of a data breach where their personal information is being used to file fraudulent unemployment claims, along with credit card fraud. Currently, officials at the county are not clear if this breach happened internally or by external hackers.

March 3, 2014 City of Detroit, Michigan

The City of Detroit announced a security breach that affected files of approximately 1,700 city employees. Apparently the breach occurred when an employee clicked on a software link that contained malicious software that released a code that froze access to numerous files.

The files included names, birth dates and Social Security numbers of current and former city employees.
Affected records: 1,700 (≈ $292,400)

Source: https://www.privacyrights.org/data-breach

Information Security

Last Updated: 14-Sep-2014

Information is power, just ask:

- Google
- People who stole all that card info from Target, PF Changs, Harbor Freight and now Home depot (and numerous)others
- People who had their identity stolen
- People who black mail others

Information Security

Last Updated: 14-Sep-2014

Information in the wrong hands, just like power, is dangerous. We deal with information every day:

- News, gossip, rumors
- Payroll and Social Security data
- Tax assessments, rolls, liens etc.
- Legal decisions
- Company or state secrets (and everything in between)
- Health information
- Personal and personnel data

Information Security

Last Updated: 14-Sep-2014

Sometimes the information is our own, sometimes it is about or from complete strangers, and sometimes about companies, villages, towns, cities, counties, states, fire districts, hospitals …

The majority of information nowadays is kept electronically – who here does NOT use online banking? Shopping? Social Media like Facebook, Twitter, or LinkedIn?

Information Security deals with keeping that information safe – from the wrong hands.

Information Security

Last Updated: 14-Sep-2014

Information (or data) are kept electronically on:

- Computer disks
- Removable media (USB sticks, CD/DVD, tape, floppies, punch cards (???)
- Phones
- ...

Information (or data) are kept physically on:

- Computers, phones, data center, cloud
- Paper (printouts, post-it-notes, etc.)

Information Security

Last Updated: 14-Sep-2014

Criminals know about the value of information – that is why they try to access or steal it.

Access to data is usually provided to authorized persons only – so thieves try to get that access from these persons or try to impersonate them.

Criminals use fake emails, false web sites, or simply phony identities (e.g. in a phone call to the help desk).

Criminals use brute-force attacks to get access to data via password, unsecured access methods (e.g. database without a password, appliance with a default password).

Information Security

Last Updated: 14-Sep-2014

According to the 2014 report on the cost of data breaches published by the Ponemon Institute and IBM, the cost of a data breach is $172 per capita for the "Public" sector ... a breach affecting 5,000 records (e.g. voter registrations) will incur a cost of $860,000!

Breaches in Healthcare cost approx. $372 per capita ... counties or cities with health facilities can expect even higher costs in such a case.

The likelihood of small breaches (at most 10,000 records affected) over the next two years is 19%, large breaches (100,000 or more records) are expected to occur at 0.8% probability.

In comparison, the likelihood to win jackpot in the state lottery is 1 in 45 millions [= 0.00000222222222222225%] (http://nylottery.gov).

Information Security

Last Updated: 14-Sep-2014

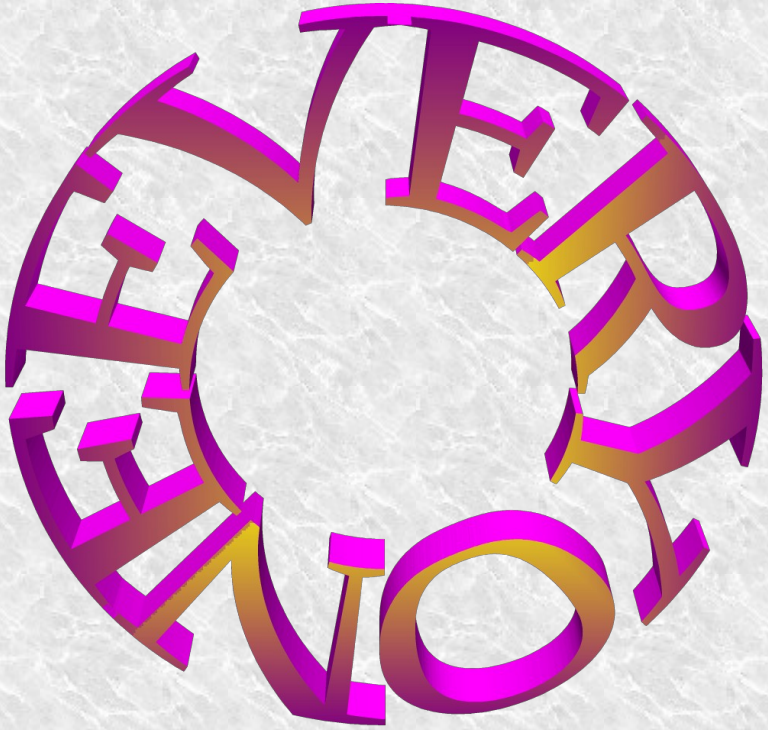
We need to protect information – be it our own or others:

- Strengthen the weakest link (i.e. human) via a formal ***Security Awareness Program***
- Determine value and probability of data breaches via a ***Risk Analysis***
- Get the status of security via regular ***Security Audits*** and continuous ***Monitoring***
- Deploy defense in depth measures like ***Network and Application Firewalls, IDS/IPS systems, Log Analyzers, Automatic Alerts***
- Have security policies in place and enforce them: ***http://www.sans.org/security-resources/policies***

Information Security

Last Updated: 14-Sep-2014

Who is responsible for Information Security?



EVERYONE !