April 18, 2014 Release # 262

Begin Transmission…

DATA THEFT, the deliberate stealing of information, rather than its accidental loss.

It can take place both inside an organization (e.g., by a disgruntled employee), or by criminals outside the organization.

Criminals often use malware to access a computer and steal data. A common approach is to use a Trojan to install keylogging software that tracks everything the user types, including usernames and passwords, in order to access the user's bank account.

In 2013, for example, names, Social Security numbers and other sensitivie data about individuals involved in pending court cases were stolen from the State of Washington Administrative Office of the Courts.

Some other recent data thefts include some of the biggest in history:

Email marketing company Epsilon leaks millions of names and email addresses from customer databases of Best Buy, Marks & Spencer and Chase Bank. Initial cost containment and remediation is estimated at $225M, but could reach as high as $4B.

Servers are breached for Global Payments, a payments processor for Visa, exposing information on as many as 7M card holders.

Over 50 million names, email addresses, and encrypted passwords are stolen from LivingSocial, a popular daily deals website.

2011 **2011** **2011** **2012** **2013**

Sony Corp suffers breaches that place 100M customer accounts at risk, costing the company up to $2 billion.

More than 6 million poorly encrypted LinkedIn passwords are published on an underground criminal website.

Data Theft also occurs when devices containing data, such as laptops or USB drives, are stolen.

End of Transmission…

Information Security: It's a Shared Responsibility
REFERENCE(S): Sophos Threatsaurus : The A-Z of Computer and Data Security Threats
INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.