SOS CHILDREN'S VILLAGES INTERNATIONAL

Digital Revolution calls for comprehensive security solutions

Accountable Now 2016, Webinar

Oliver Vavtar

Team Leader Network Services
Information and Communication Technology
SOS Children's Villages International
Hermann-Gmeiner-Str. 51
6020 Innsbruck

Tel.: +43 512 3310 5147
oliver.vavtar@sos-kd.org
www.sos-childrensvillages.org

SOS CHILDREN'S VILLAGES INTERNATIONAL

Opening

In the **age of always connected** mobile devices, social networks and **new consumer behaviours**, the **IT security department has an increasing important role for organizations across all sectors**.

Attackers are **more organized**, **attacks** are **more sophisticated** and **threats** are **more dangerous than ever before**.

This session shows several **examples of actual threats** and describes the **approach of SOS how to overcome those security challenges** these days and in the future.

SOS CHILDREN'S VILLAGES INTERNATIONAL

Introduction

Oliver Vavtar

SOS Children's Villages International

Team Leader Network Services

Oliver Vavtar is Team Leader Network Services for SOS Children's Villages International where he and his team is involved in all aspects of global Service Delivery including Communications Infrastructure, Information Security Management, Business Continuity Management and Network Architecture and Operation.Oliver graduated in telecommunication engineering and electronics, has more than 20 years of experience in ICT, is a seasoned leader for local and global teams and is a member of ICT management team of the General Secretariat of SOS Children's Villages International.

tirol Unser Land

BRITISH AIRWAYS

SOS CHILDREN'S VILLAGES INTERNATIONAL

Threats can come from any direction…

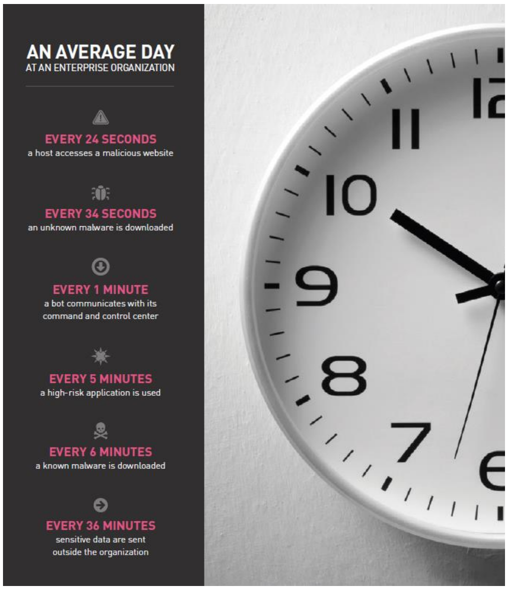
… and it has become impossible to say that any one organization is safe from attack.

In fact, the biggest mistake any organization can make is to believe it is protected.

"The Cold War didn't end in the 1990s. It simply moved online."[31]

-Jose Pagliery, journalist

An average day in a company…



AN AVERAGE DAY
AT AN ENTERPRISE ORGANIZATION

EVERY 24 SECONDS
a host accesses a malicious website

EVERY 34 SECONDS
an unknown malware is downloaded

EVERY 1 MINUTE
a bot communicates with its command and control center

EVERY 5 MINUTES
a high-risk application is used

EVERY 6 MINUTES
a known malware is downloaded

EVERY 36 MINUTES
sensitive data are sent outside the organization

!

Source: Check Point Technologies

Popular threats...

Organized crime

- or terrorist groups using identity theft and other forms of compromise or extortion (e.g. denial of service attacks)

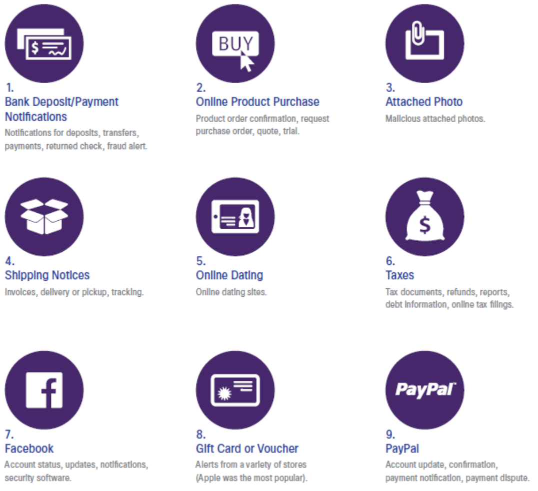
Malware authors

- responsible for Viruses, Worms, Trojans (particularly key loggers)

Phishing

- including spear phishing targeting individuals with carefully crafted attacks

Popular threats...



1. **Bank Deposit/Payment Notifications**
Notifications for deposits, transfers, payments, returned check, fraud alert.

2. **Online Product Purchase**
Product order confirmation, request purchase order, quote, trial.

3. **Attached Photo**
Malicious attached photos.

4. **Shipping Notices**
Invoices, delivery or pickup, tracking.

5. **Online Dating**
Online dating sites.

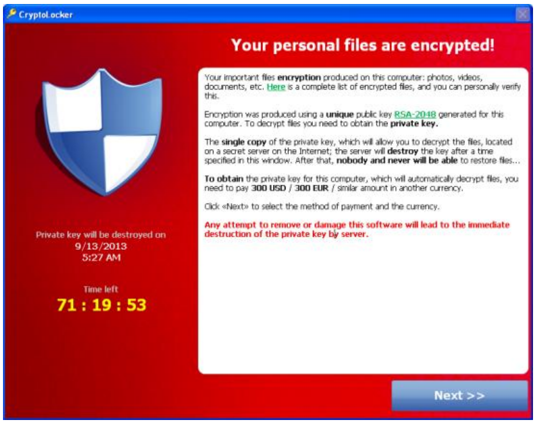
6. **Taxes**
Tax documents, refunds, reports, debt information, online tax filings.

7. **Facebook**
Account status, updates, notifications, security software.

8. **Gift Card or Voucher**
Alerts from a variety of stores (Apple was the most popular).

9. **PayPal**
Account update, confirmation, payment notification, payment dispute.

Popular threats...



CryptoLocker

Your personal files are encrypted!

Private key will be destroyed on
9/13/2013
5:27 AM

Time left
71 : 19 : 53

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>

Ransomware

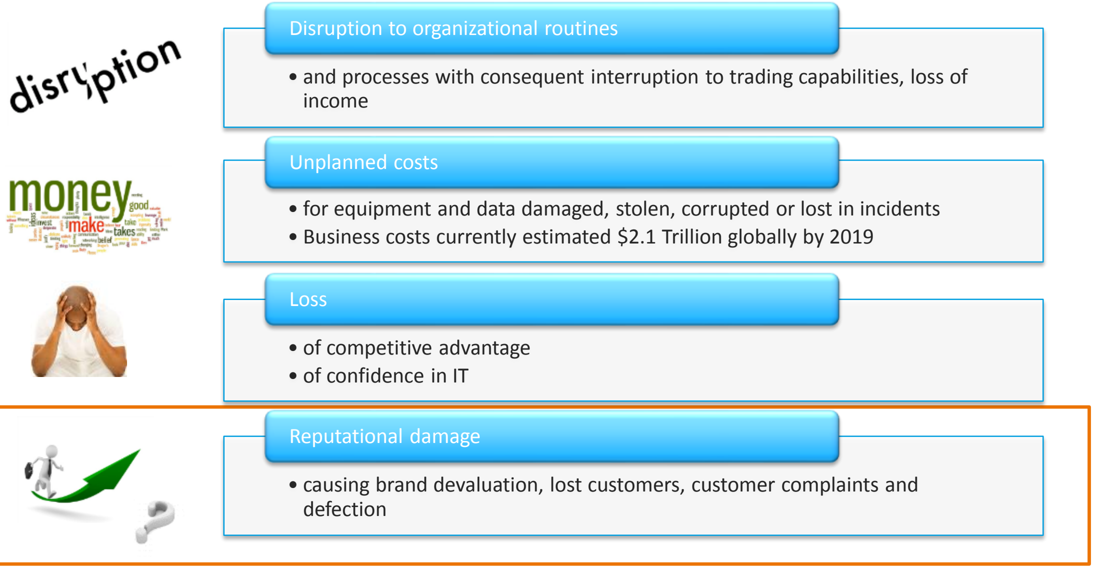
- spreads through e-mail attachments, infected programs and compromised websites
- to extort money
- after a victim discovers he cannot open a file, he receives an email ransom note demanding an amount of money in exchange for a private key

External threats only?

So called **insider threats** are still the most prevalent cyber-attack vector

→ **55% of all attacks** are carried out by **malicious insiders or inadvertent actors**

Which impacts could result from attacks



Disruption to organizational routines

- and processes with consequent interruption to trading capabilities, loss of income

Unplanned costs

- for equipment and data damaged, stolen, corrupted or lost in incidents
- Business costs currently estimated $2.1 Trillion globally by 2019

Loss

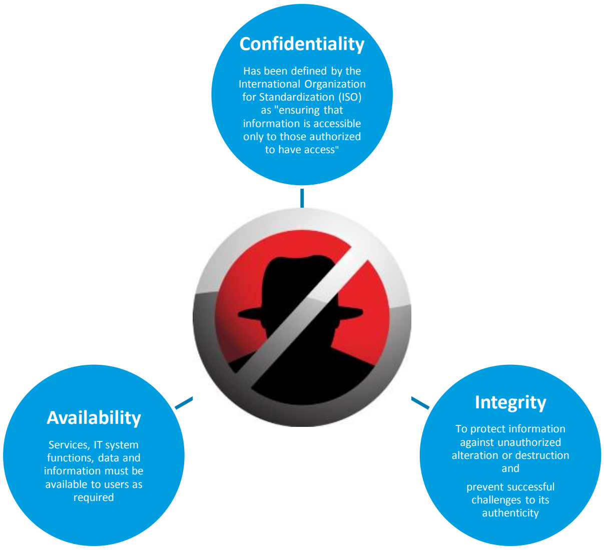
- of competitive advantage
- of confidence in IT

Reputational damage

- causing brand devaluation, lost customers, customer complaints and defection

SOS CHILDREN'S VILLAGES INTERNATIONAL

Main pillars of information security



Confidentiality

Has been defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorized to have access"

Availability

Services, IT system functions, data and information must be available to users as required

Integrity

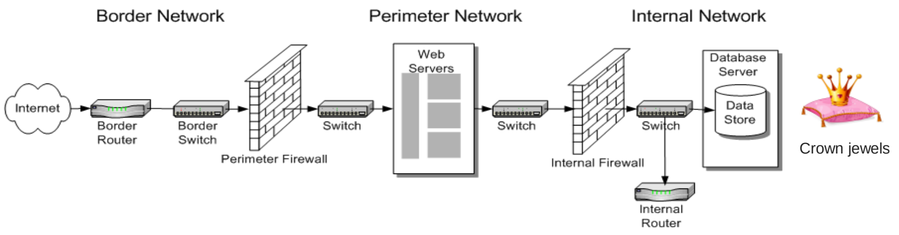
To protect information against unauthorized alteration or destruction and

prevent successful challenges to its authenticity

SOS CHILDREN'S VILLAGES INTERNATIONAL

I miss those days…

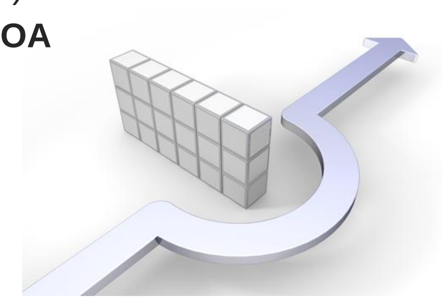
- Traditional Security Approach
  - Perimeter (on prem fw with UTM, antivirus, disk encryption, DLP, anti spyware, SSL, Privileged Identity Management, IDS/IPS, etc.)

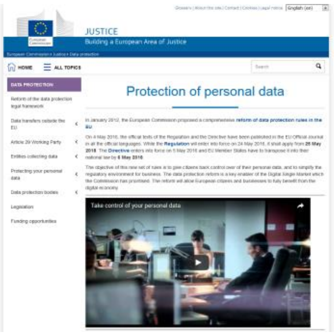


SOS CHILDREN'S VILLAGES INTERNATIONAL

The situation nowadays…

- **Collaboration** – within and especially **outside the organization** (partner, customer, supplier, etc.)
- **Sensitive information leaves the organization every day** (mobility and external storing, outsourcing, stored in the cloud, given to other people, etc.)
- **BYOD, BYOA**





Glossary | About this site | Contact | Cookies | Legal notice English (en)

European Commission

JUSTICE

Building a European Area of Justice

European Commission > Justice > Data protection

HOME ALL TOPICS Search

DATA PROTECTION

- Reform of the data protection legal framework
- Data transfers outside the EU
- Article 29 Working Party
- Entities collecting data
- Protecting your personal data
- Data protection bodies
- Legislation
- Funding opportunities

Protection of personal data

In January 2012, the European Commission proposed a comprehensive **reform of data protection rules in the EU**.

On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the **Regulation** will enter into force on 24 May 2016, it shall apply from **25 May 2018**. The **Directive** enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by **6 May 2018**.

The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritised. The reform will allow European citizens and businesses to fully benefit from the digital economy.

Take control of your personal data

SOS CHILDREN'S VILLAGES INTERNATIONAL

New security challenges

How to overcome new threats and how to be brought in compliance with the law?

Approach of SOS, considerations

- **Security** as a **Social Norm**
  - The main **ingredients of success** are
    - well aligned **technology**,
    - well deliberated **organizational procedures** and
    - reliable, **well informed staff fulfilling their security obligations** - from **upper management** across other functions to **ICT experts**

Approach of SOS, considerations

- Bear in mind the **human factor**
  - **Technical measures alone** cannot achieve the best possible reliability, and **will never achieve trustworthiness**
  - **All** users **need to be educated** in the part they have to play in the security of the systems they own; through learning and **following good practice**
  - **Awareness** - People are the most important part of information safety

SOS CHILDREN'S VILLAGES INTERNATIONAL

Approach of SOS, considerations

- **Stay focused** and **stay ahead**
  - **Cybercriminals** aren´t teenagers; they **are perfectly organized** and **highly specialized on stealing PII and intellectual property**
  - **Information security leadership needs to be vigilant**
  - **Traditional security management** simply **isn´t agile enough** to deal with the perils of cyber activity

SOS CHILDREN'S VILLAGES INTERNATIONAL

Approach of SOS, considerations

- **Involve each department** operating with sensitive data
  - THEY know exactly
    - **WHO** should use information,
    - **WHAT** should be done with information,
    - **WHEN and WHERE** should information be accessed/used

SOS CHILDREN'S VILLAGES INTERNATIONAL

Approach of SOS, considerations

- **User acceptance** is key
  - Data security measures **need to be easy to understand and viable** for the users
  - Provide **smart training materials (intranet, webinars, f2f interaction, e-learning, clips, quiz games, etc.) but do not spam them** ☺

Show them the way, but **try to get rid of topic responsibility – ICT ≠ data protection!**

SOS CHILDREN'S VILLAGES INTERNATIONAL

Last slide…

- **THX** for your attention ☺