From bullet point journal to lessons learned

How to manage coordination and cooperation development in ad-hoc working environment

Agenda

- What we do @ NCSC-FI?
- How we do it?
  - » **Bullet point journal**
- How do we improve it?
  - » **Lessons learned**

Warning!

This presentation is not technical and does not have any technical details!

It is about handling the flow of technical cases

What we do?

NCSC-FI as an operational team

TLP: white

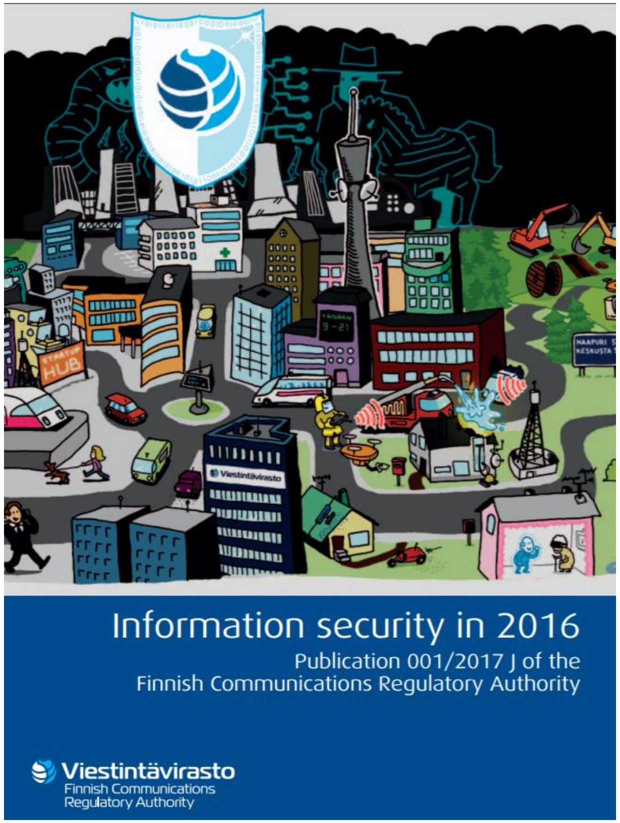
Incidents handled yearly

Incident reports per year	
Incident reports	Over 1000
Vulnerability coordination	Over 10
NCSC-FI monitoring systems	
Autoreporter	50 - 410 000
HAVARO	Over 100

TLP: White

Publications yearly

Public	
Blog posts	**80**
Facebook & Twitter	**Over 100**
Distribution lists	
Week reports	**52**
Monthly summaries	**12**
Daily news letters	**360**
Vulnerability letters	**99** (from june 2016)
CIP-messages	**238**



Information security in 2016

Publication 001/2017 J of the
Finnish Communications Regulatory Authority

Viestintävirasto
Finnish Communications
Regulatory Authority

TLP: white

1 duty officer /1week

- Incident response 24/7/365
- triage
- News follow up

2 duty officer /1week

- Blog posts
- Aids 1. duty officer

Coordinator/3weeks

- Coordinates significant incidents
- Follows and coordinates situation awereness

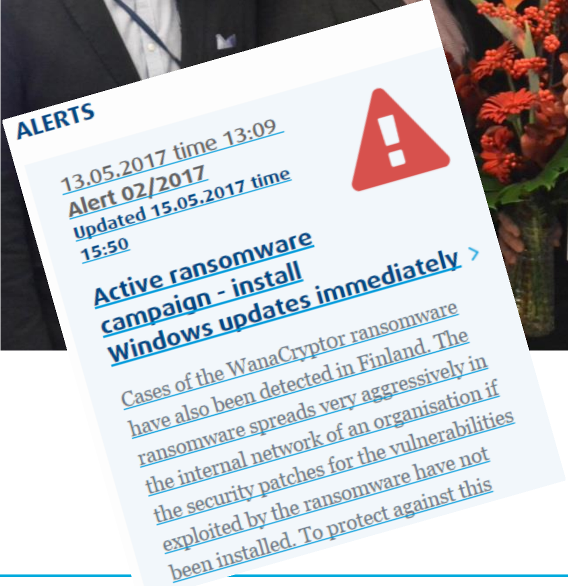
3 duty officer /1week

- HAVARO monitoring

"CERT Public announcements" awarded as information security phonemon of the year 2016

TLP: white

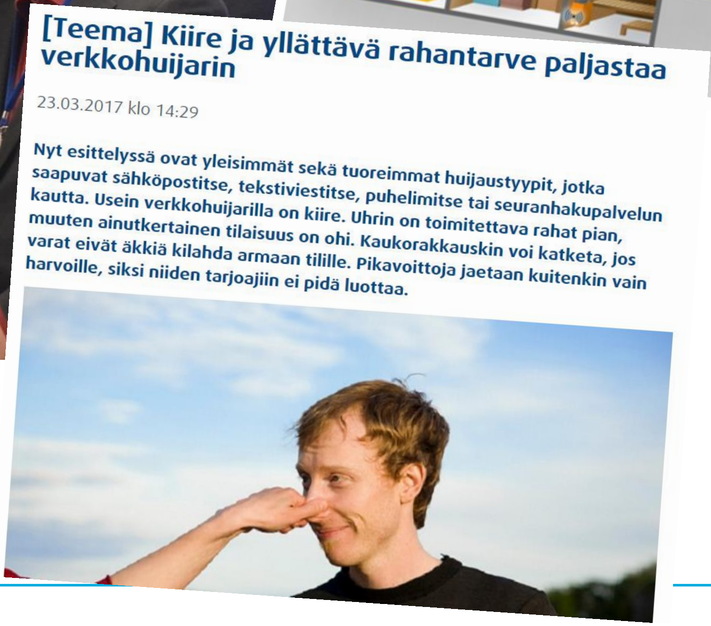
BITTI
VUODEN TUOTE
Vuoden 2016 tietoturvailmiö
Kyberturvallisuuskeskus, CERT-toiminta


ALERTS

13.05.2017 time 13:09
Alert 02/2017
Updated 15.05.2017 time 15:50

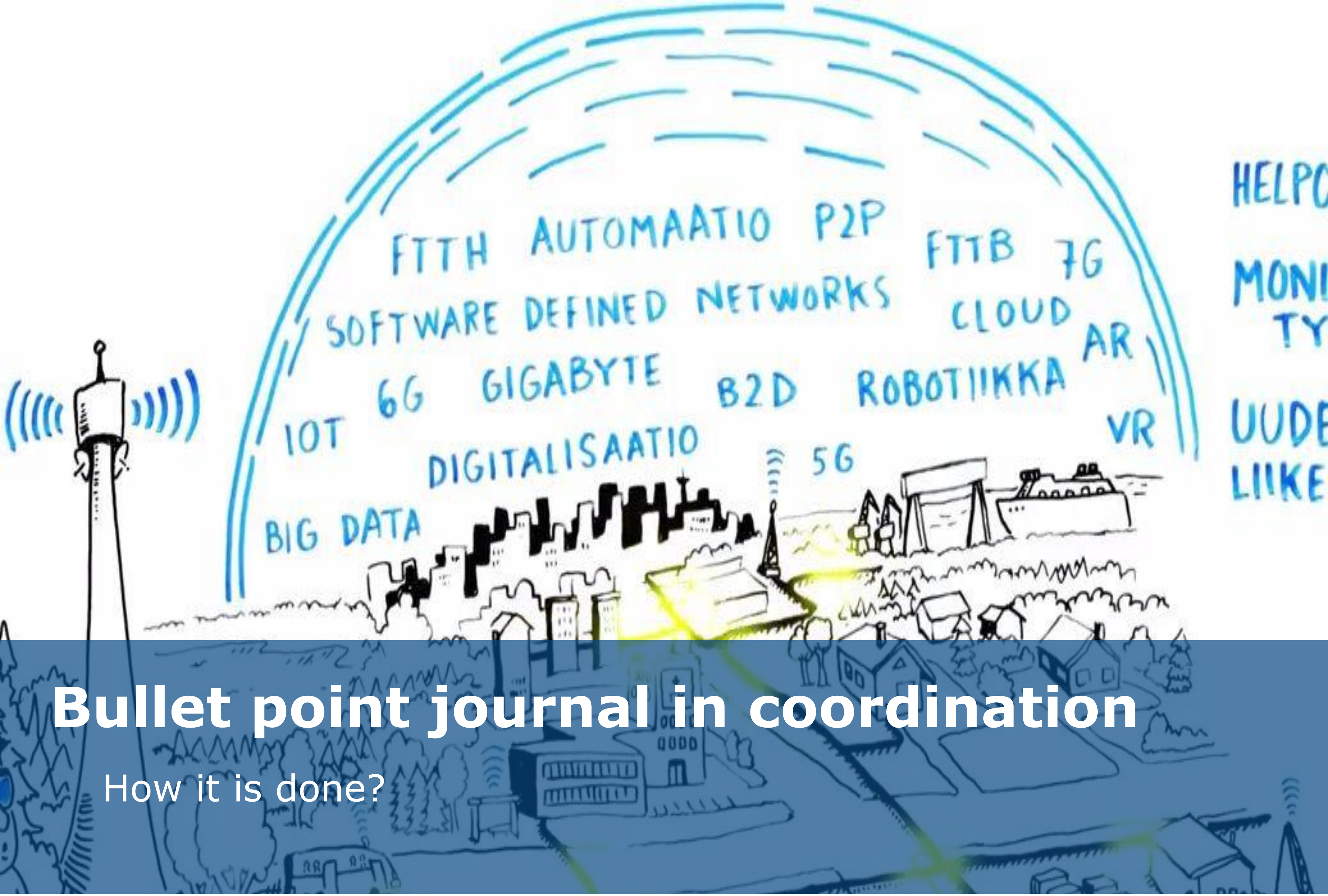
Active ransomware campaign - install Windows updates immediately

Cases of the WanaCryptor ransomware have also been detected in Finland. The ransomware spreads very aggressively in the internal network of an organisation if the security patches for the vulnerabilities exploited by the ransomware have not been installed. To protect against this


[Teema] Kiire ja yllättävä rahantarve paljastaa verkkohuijarin

23.03.2017 klo 14:29

Nyt esittelyssä ovat yleisimmät sekä tuoreimmat huijaustyypit, jotka saapuvat sähköpostitse, tekstiviestitse, puhelimitse tai seuranhakupalvelun kautta. Usein verkkohuijarilla on kiire. Uhrin on toimitettava rahat pian, muuten ainutkertainen tilaisuus on ohi. Kaukorakkauskin voi katketa, jos varat eivät äkkiä kilahda armaan tilille. Pikavoittoja jaetaan kuitenkin vain harvoille, siksi niiden tarjoajiin ei pidä luottaa.



Bullet point journal in coordination

How it is done?

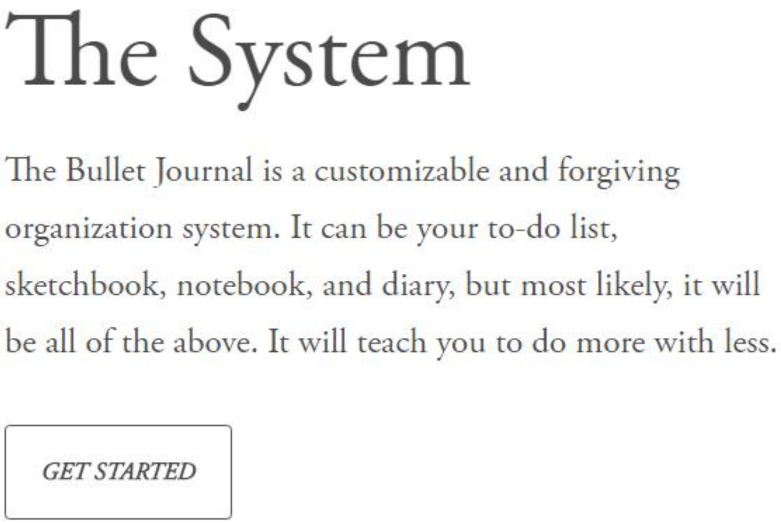
Problems and questions

1. Mostly ad-hoc cases
2. Obtained from variety of sources
3. All having different kind of problems
4. Several people handling them
5. With many cooperation parties

1. **What is important and to whom?**
2. **What to follow for longer?**
3. **What is the overall situation?**
4. **Where is it going?**
5. **Did we do it correctly?**

TLP: white

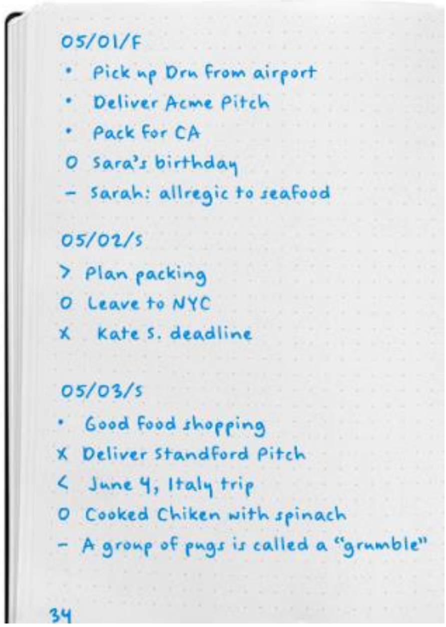
What is a bullet point journal?



The System

The Bullet Journal is a customizable and forgiving organization system. It can be your to-do list, sketchbook, notebook, and diary, but most likely, it will be all of the above. It will teach you to do more with less.

GET STARTED



05/01/F

• Pick up Dru from airport

• Deliver Acme Pitch

• Pack for CA

O Sara's birthday

– Sarah: allregic to seafood

05/02/S

> Plan packing

O Leave to NYC

X Kate S. deadline

05/03/S

• Good food shopping

X Deliver Standford Pitch

< June 4, Italy trip

O Cooked Chiken with spinach

– A group of pugs is called a "grumble"

34

Source: www.bulletjournal.com

❑ **From "Big Picture" to "small details"**
❑ **Aid with topics and symbols**

TLP: white

Cyberweather follows 6 topics

- □ Espionage
- □ DDoS
- □ Malware and Vulnerabilities
- □ Fraud & Phishing
- □ Network Functionality
- □ IoT

TLP: green

Daily (morning brief)

□ New cases

□ Topic news

□ Vulnerabilities

□ IOC's data

□ Monitoring systems

□ Customer contacts & networks

Weekly (report)

□ Espionage

□ DDoS

□ Malware and vulnerabilites

□ Fraud & Phishing

□ Network functionability

□ IoT

Monthly (trends)

□ Cyberweather collage

□ Update of statistics and trends

Yearly (year book)

□ Summary & Forecast

□ Analyze: TOP5 threats and solutions

Bullet point journal @ NCSC-FI?

#cyberweather in May2017

Worldwide problems from aggressive WannaCry –ransomware

Espionage

- Affecting elections worries all over Europe
- ICT-service providers as a spread vector to organizations

Denial of service

- Gigabit DDoSes everyday in Finland
- Several notifications of threatening with DDoSes

Fraud & Phishing

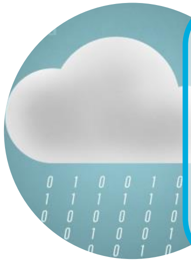
- Continues bank and Apple ID phishing has become new normal
- Subscription traps common

Malware and vulnerabilities

- WannaCry ransomware spread all over world
- Finland suffered few hits

Functionality of communication services

- No significant disturbances lately
- Significantly less disturbances than year ago



IoT

- Minimum requirements discussed in EU level
- Scanning industrial control systems 2017 revealed unprotected critical devices in network
- .

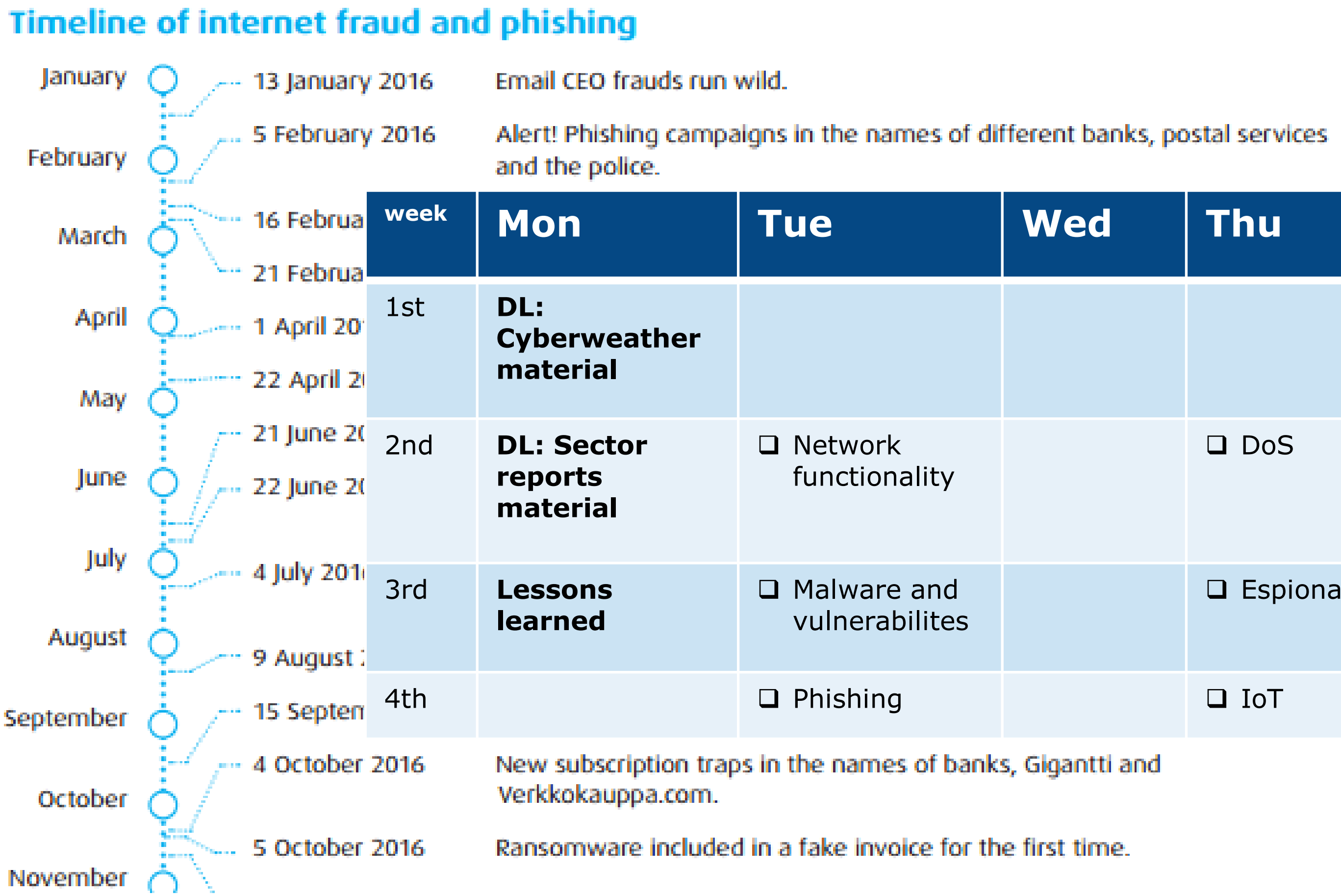
TLP: green

NCSC-FI daily week timetable

	Mon	Tue	Wed	Thu	Fri
Daily	**Morning brief (coordinator)**	**Morning brief (coordinator)**	**Morning brief (coordinator)**	**Morning brief (coordinator)**	**Shift of duty (1. duty officer)**
Report				***Weekly report*** *- AMBER*	***Weekly report*** *- GREEN*
Work	**Group meetings**				**NCSC-FI meeting**

TLP: green

NCSC-FI weekly month timetable



Timeline of internet fraud and phishing

January
February
March
April
May
June
July
August
September
October
November

13 January 2016 Email CEO frauds run wild.

5 February 2016 Alert! Phishing campaigns in the names of different banks, postal services and the police.

16 Februa

21 Februa

1 April 20

22 April 2

21 June 2

22 June 2

4 July 201

9 August

15 Septen

4 October 2016 New subscription traps in the names of banks, Gigantti and Verkkokauppa.com.

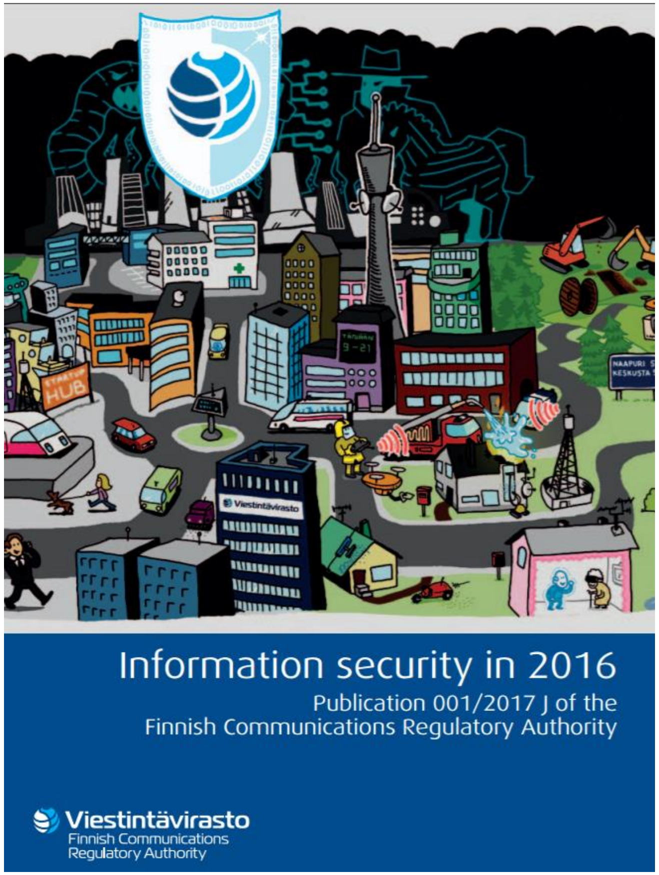
5 October 2016 Ransomware included in a fake invoice for the first time.

week	Mon	Tue	Wed	Thu	Fri
1st	**DL: Cyberweather material**				**Update: Cyber-weather**
2nd	**DL: Sector reports material**	□ Network functionality		□ DoS	**Sector reports**
3rd	**Lessons learned**	□ Malware and vulnerabilites		□ Espionage	
4th		□ Phishing		□ IoT	

TLP: white

All gathers to a Year Book

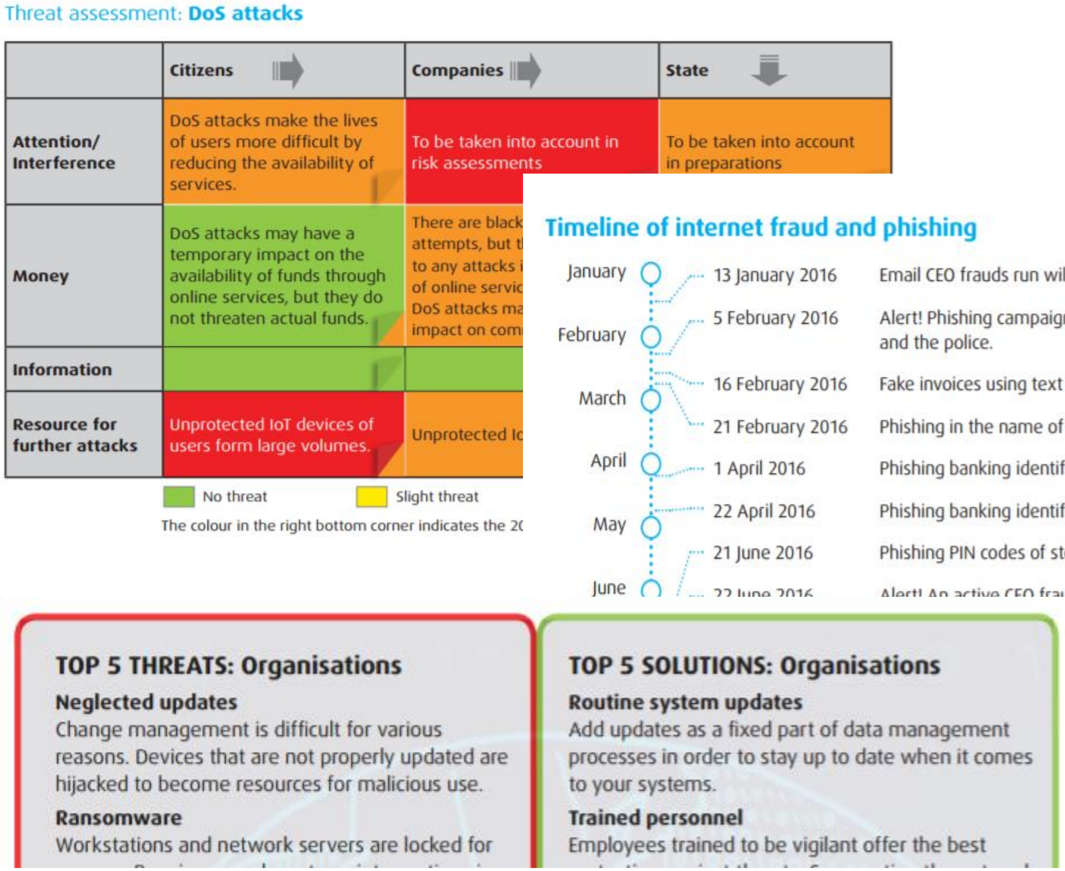
https://www.viestintavirasto.fi/attachments/tietoturva/Information_Security-2016_ViVi-27-03.pdf



Information security in 2016

Publication 001/2017 J of the
Finnish Communications Regulatory Authority

Viestintävirasto
Finnish Communications
Regulatory Authority



Threat assessment: **DoS attacks**

	Citizens	Companies	State
Attention/ Interference	DoS attacks make the lives of users more difficult by reducing the availability of services.	To be taken into account in risk assessments	To be taken into account in preparations
Money	DoS attacks may have a temporary impact on the availability of funds through online services, but they do not threaten actual funds.	There are black attempts, but t to any attacks i of online servic DoS attacks ma impact on com	
Information			
Resource for further attacks	Unprotected IoT devices of users form large volumes.	Unprotected Io	

🟩 No threat 🟨 Slight threat

The colour in the right bottom corner indicates the 20

Timeline of internet fraud and phishing

13 January 2016	Email CEO frauds run wild.
5 February 2016	Alert! Phishing campaigns i and the police.
16 February 2016	Fake invoices using text me
21 February 2016	Phishing in the name of th
1 April 2016	Phishing banking identifier
22 April 2016	Phishing banking identifier
21 June 2016	Phishing PIN codes of stole
22 June 2016	Alert! An active CEO fraud

TOP 5 THREATS: Organisations

Neglected updates

Change management is difficult for various reasons. Devices that are not properly updated are hijacked to become resources for malicious use.

Ransomware

Workstations and network servers are locked for

TOP 5 SOLUTIONS: Organisations

Routine system updates

Add updates as a fixed part of data management processes in order to stay up to date when it comes to your systems.

Trained personnel

Employees trained to be vigilant offer the best

Lessons learned

Improving the way of work

TLP: white

What is lessons learned?

http://www.projectmanagers.net/i/top-mistakes-in-project-management/you-will-make-mistakes/

TLP: white

Lessons learned in action

Improvement ideas and feed back brought up by the employees

- Once a month held discussion session
- 2-4 cases picked up brought up by the employees
- What did we do right/wrong?
  - Improvement ideas listed
  - Taken to management
  - Management decides what ideas are taken into actions to improve future way of work

TLP: white

Results of lessons learned 2016

22 cases discussed

In **9** sessions

We found

- **75 ideas**!
- Many success stories

TLP: white

Conclusions

- **Simplify** - with simple topics
- **Check points** - for freedom of doing in ad-hoc
- **Learn** - from the mistakes and successes!

Finnish Communications Regulatory Authority

National Cyber Security Centre

Jarna.hartikainen@ficora.fi

www.ncsc.fi
www.ficora.fi