
Finnish Communications
Regulatory Authority
cert-fi
Incident Reporting
in Finland
2009-10-23
ENISA & EDPS
Erka Koivunen
Head of CERT-FI
Finnish Communications
Regulatory Authority

Finnish Communications Regulatory Authority

Incident Reporting ☒

Data Breach Reporting ☐

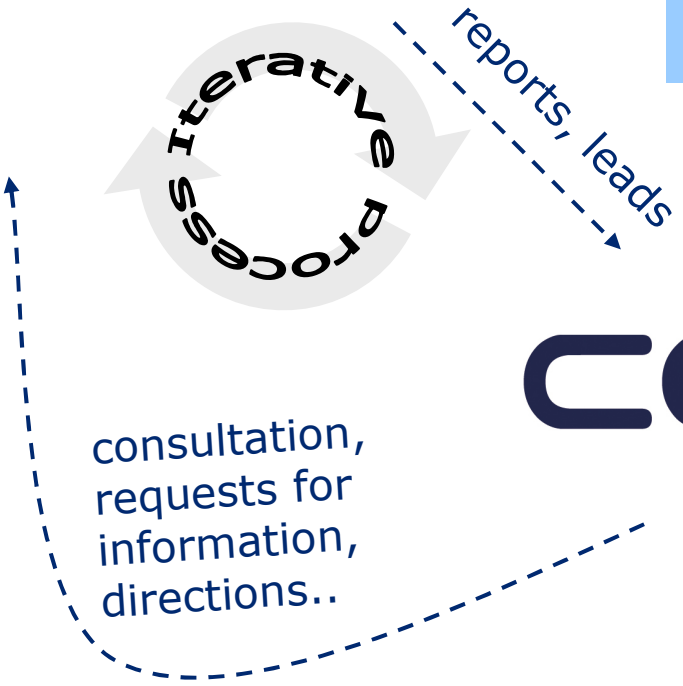
Special about the Finnish model..

dna TDC FINNET etc..

TeliaSonera

elisa

Telecommunications operators



cert-fi

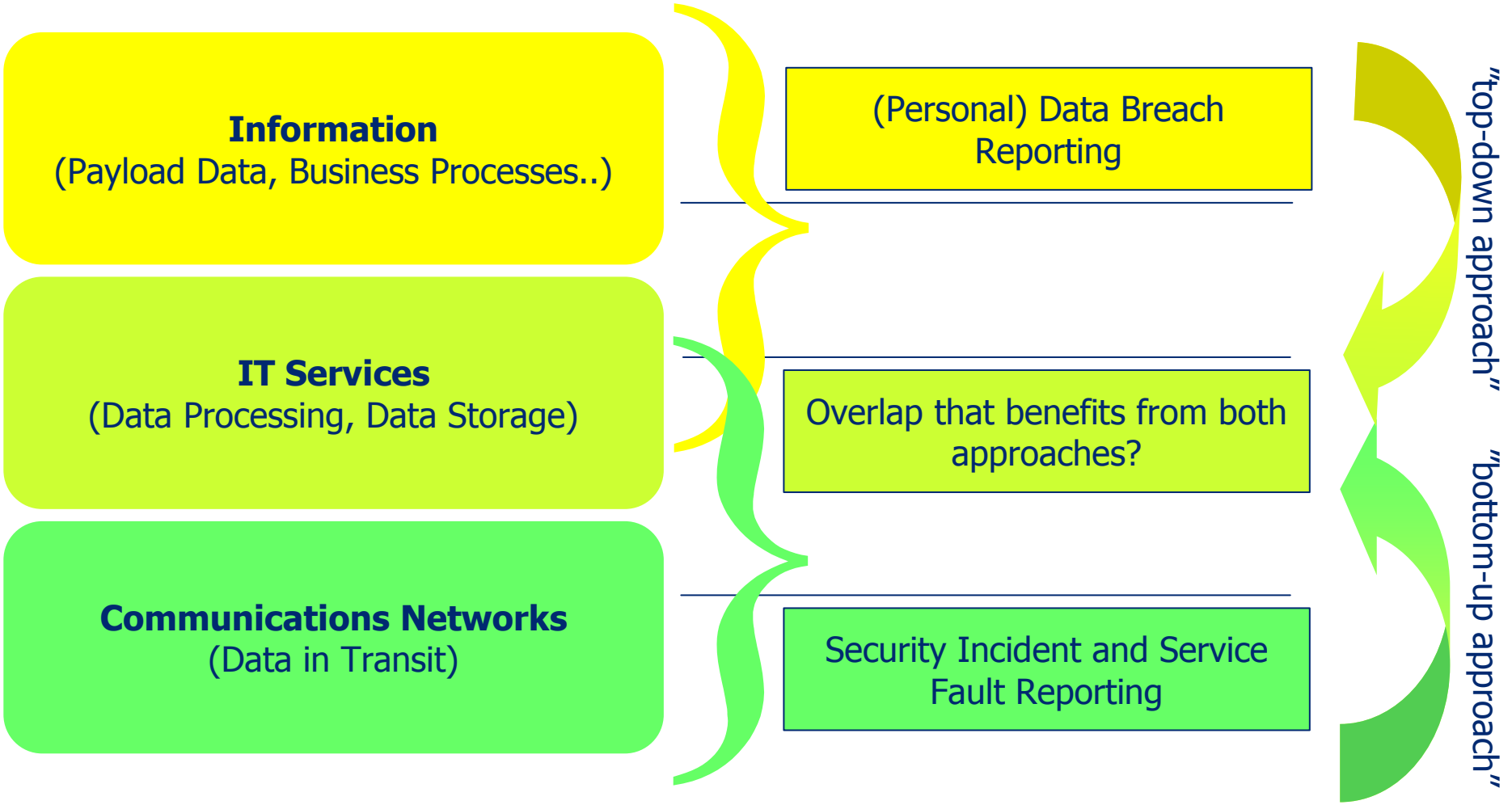
Viestintävirasto
Kommunikationsverket
Finnish Communications Regulatory Authority

Applies to Telecommunications Operators only:

Mandatory reporting of Information Security Incidents as well as Major Faults:

- affecting the networks
- affecting users of the networks
- affecting service provider's ability to operate it's networks

Security Incident vs. Data Breach



To report or not? And what to whom?

Actors	Have duty to...		
	Protect	*Report*	*Appoint PoC*
Telecoms Providers	**X**	**authorities, subscribers**	**X**
Financial Institutions	**X**	**authorities**	**-**
Energy Companies*	**X**	**authorities**	**-**
Health Sector	**X**	**authorities**	**-**
IT Services	**X**	**-**	**-**
Government	**X**	**superiors**	**-**
Private Businesses	**X**	**-**	**-**
Other Organisations	**X**	**-**	**-**
Private Users	**-**	**-**	**-**

*) Nuclear material only

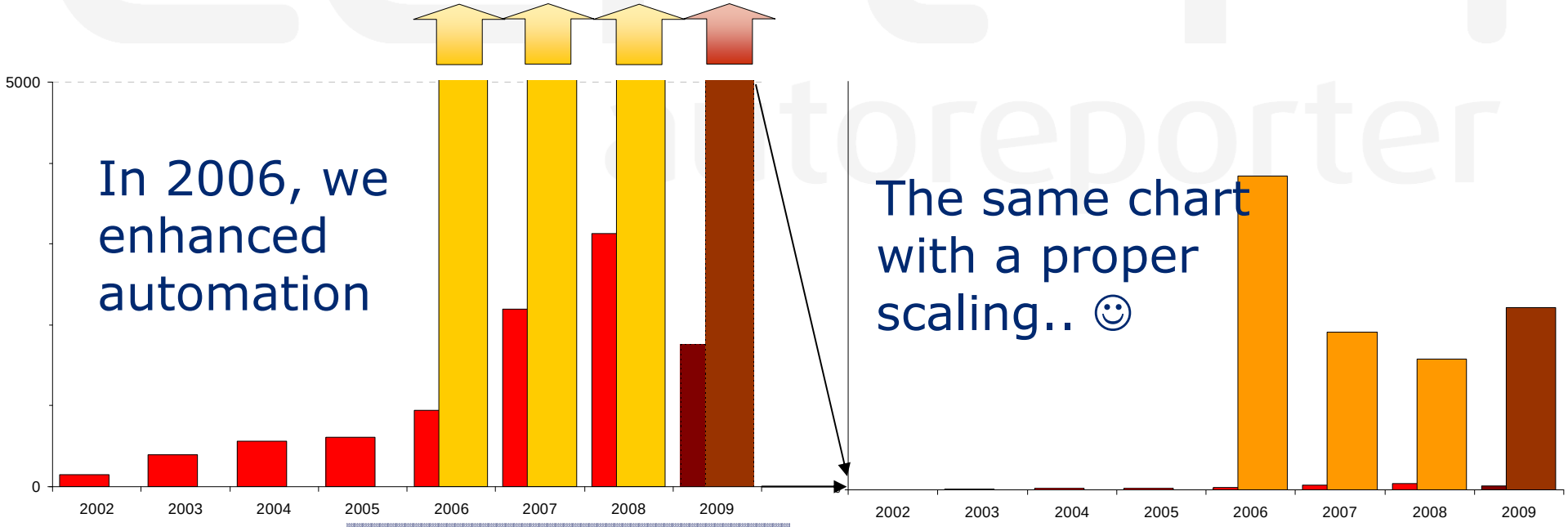
Finnish Communications Regulatory Authority

How Many Incidents

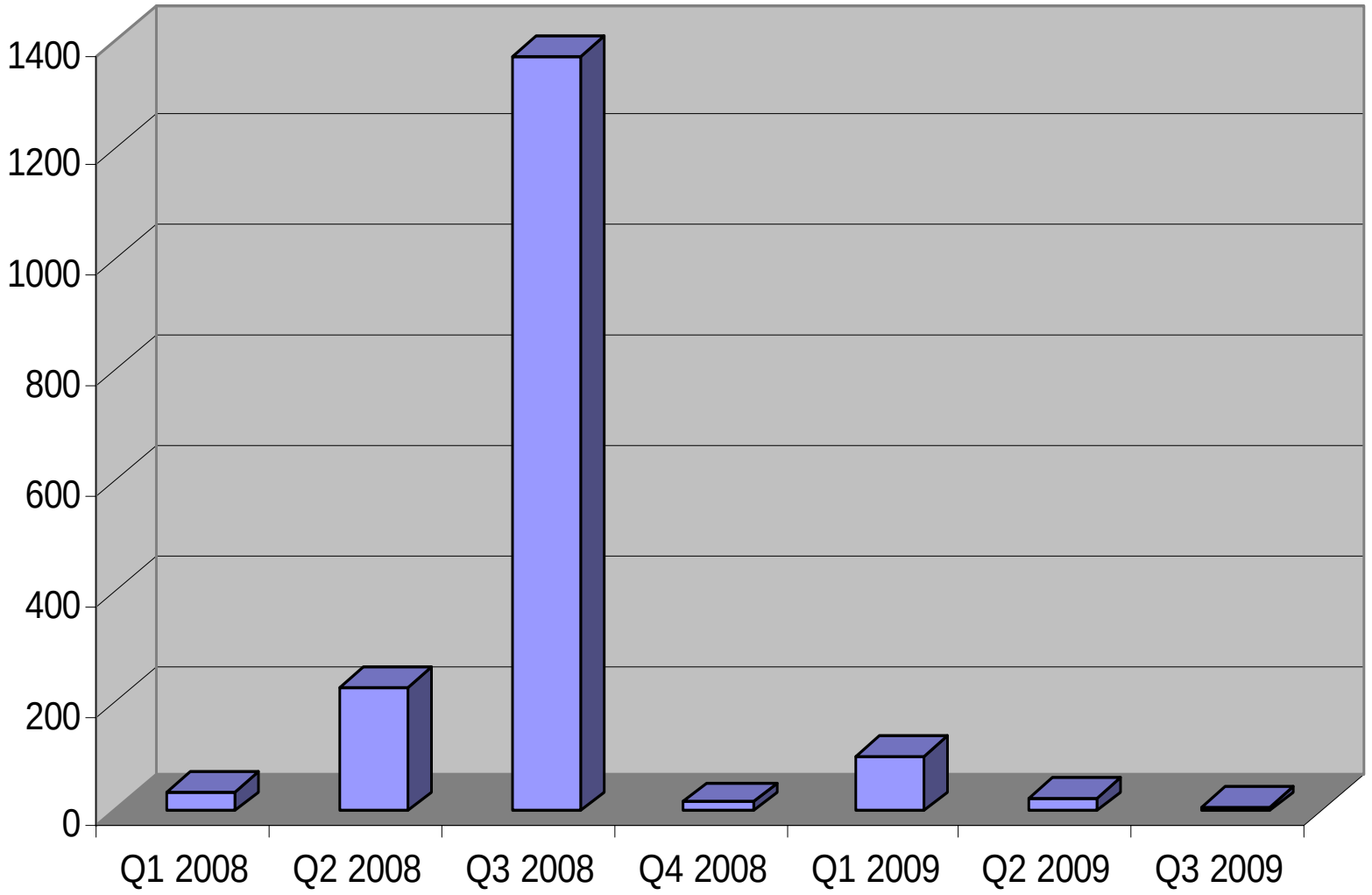
are there?

How many incidents are there?

- Since 2006, CERT-FI adopted an automated system to systematically collect Incident Reports (mostly malware infections) from various monitoring projects around the world
- **That opened our eyes!!**
- We probably still only see the tip of the iceberg..



Finnish Victims to Other Data Breach Incidents



Case: 79.000 stolen passwords

```
#define OWNED TRUE        /*  by. The Magical Pink Bear  */
                         /*       & ZeroPoint           */

#########################################################
#                                                 12/10/2007 #
# 0x00> Prologue                                          #
# 0x01> md5($password); line 68                           #
# 0x02> sha1($password); line 29934                       #
# 0x03> sha1(tolower($username) . $password); line 30352 #
# 0x04> plaintext fun; line 63122                         #
# 0x05> Goodbyes                                          #
#                                                         #
#########################################################

void Prologue()
{
    We cracked 78 000 (ok, almost 79 000) accounts around the net and
    of course we'd like to share them with you, right. Mostly finnish
    accounts, so maybe it would be better to have this prologue in
    finnish too.

        [Finnish text removed]
}


md5($password);
[REMOVED] - 913afd3bb8236e0b008a2b5590c0d996 - [REMOVED]@hotmail.com
[REMOVED] - 101186a9a44bc0354ed997696a6aefba - [REMOVED]@netti.fi
[REMOVED] - 192cf5454185eab4b02be407206e3e3c - [REMOVED]@hotmail.com
[REMOVED] - eec47280280c49e1c2d7e891e777b084 - [REMOVED]@hotmail.com
[REMOVED] - 744b4f580678b12f2db618a6a51b3fe1 - [REMOVED]@luukku.com
[REMOVED] - f0c2b1c44ad65e602106b9cbcc6b5262 - [REMOVED]@luukku.com
[REMOVED] - a68f20e7d033b008826e5486a5a3c421 - [REMOVED]@gmail.com
[REMOVED] - 5b51b91ba007bd4c22741969769bdaf7 - [REMOVED]@msn.com
```

Finnish Communications Regulatory Authority

cert-fi

In collaboration with:

National EMERGENCY SUPPLY Agency

Co-operation for the protection of critical systems

Telephone: +358 9 6966 510

E-mail: cert@ficora.fi

WWW: www.cert.fi

CERT-FI alerts and advisories are available in Finnish via:

- E-mail
- SMS (subscription fees apply)
- web pages
- RSS feed
- TELETEXT page 848 (YLE)