Grant Thornton
An instinct for growth™

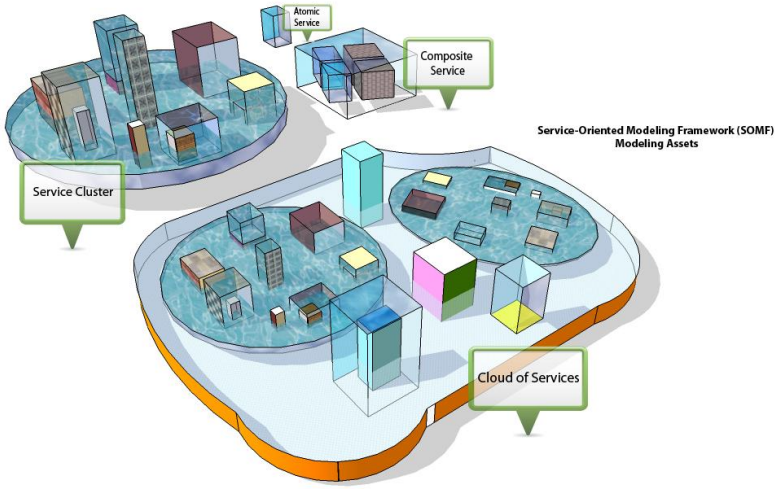
New data protection regulation

Siiri Antsmäe
Head of business risk services in Baltics
Grant Thornton Baltic
siiri.antsmae@ee.gt.com
info@ee.gt.com

Why new regulation

- speed and simplicity processing personal data
- new technology
- global excange of big data

25.05.2018



Yahoo knew of 'state-backed' hack in 2014

10 November 2016 | Technology

Share

Yahoo has confirmed that it knew for two years that a "state-sponsored actor" had hacked into its network.

In its filing, Yahoo indicates that it only discovered information from at least 500 million accounts - including names, email addresses, telephone numbers, dates of birth and unencrypted security questions and answers - had been stolen after it had looked into another unsubstantiated claim.

Deloitte hit by cyber-attack revealing clients' secret emails

Exclusive: hackers may have accessed usernames, passwords and personal details of top accountancy firm's blue-chip clients

Sept. 2017

Credit firm Equifax says 143m Americans' social security numbers exposed in hack

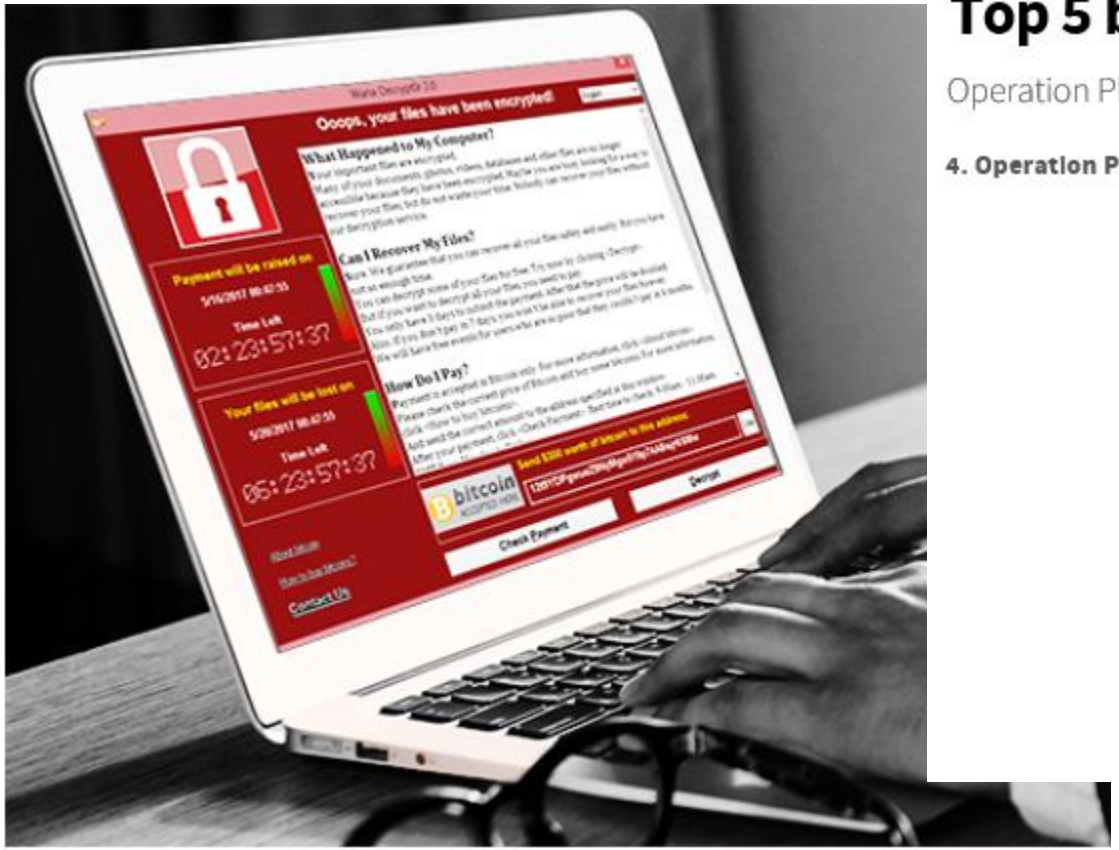
- Atlanta-based company says 'criminals' accessed personal data
- Before notifying public, Equifax executives sold $1.8m in shares

Equifax says 143 million Americans' data was breached. Photograph: Mike Stewart/AP

Credit monitoring company Equifax says a breach exposed the social security numbers and other data of about 143 million Americans.

After discovering the breach, but before notifying the public, three Equifax senior executives sold shares in the company worth almost $1.8m. Since the public announcement, the company's share price has tumbled.

Wanna Cry (May); Petya/NotPetya (June); Bad Rabbit (Oct)



Top 5 biggest phishing scams

Operation Phish Phry, RSA scammed and more

4. Operation Phish Phry

CEO fraud

From: Tom Kemp [mailto:tom.kemp@centrfiy.com]
Sent: Wednesday, September 16, 2015 8:56 AM
To: Tim Steinkopf
Subject: Payment Instruction

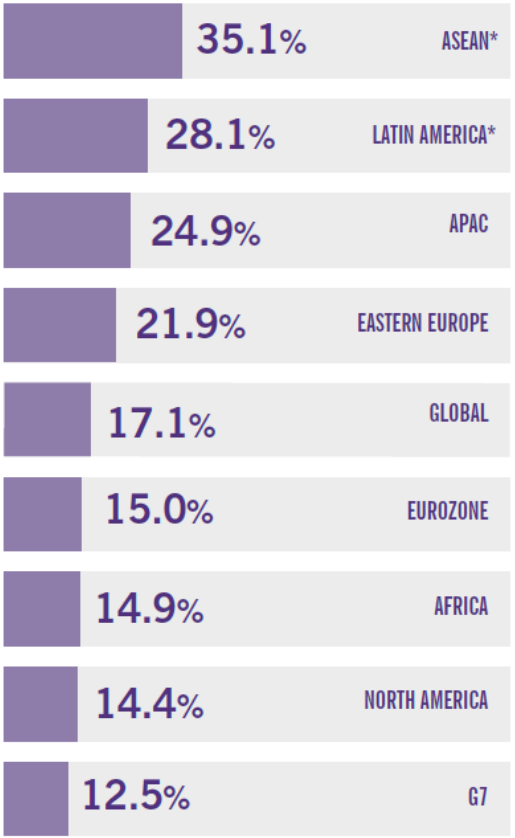
Dear Tim,

I will need you to process an urgent payment, which needs to go out today as a same value day payment.

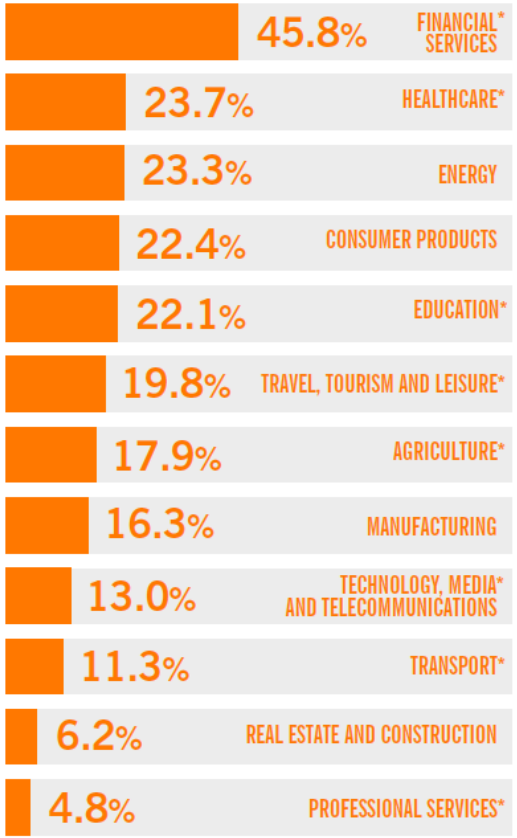
Let me know when you are set to proceed, so i can have the account information forwarded to you once received.

Extortion

EXTORTION BY REGION/GROUP



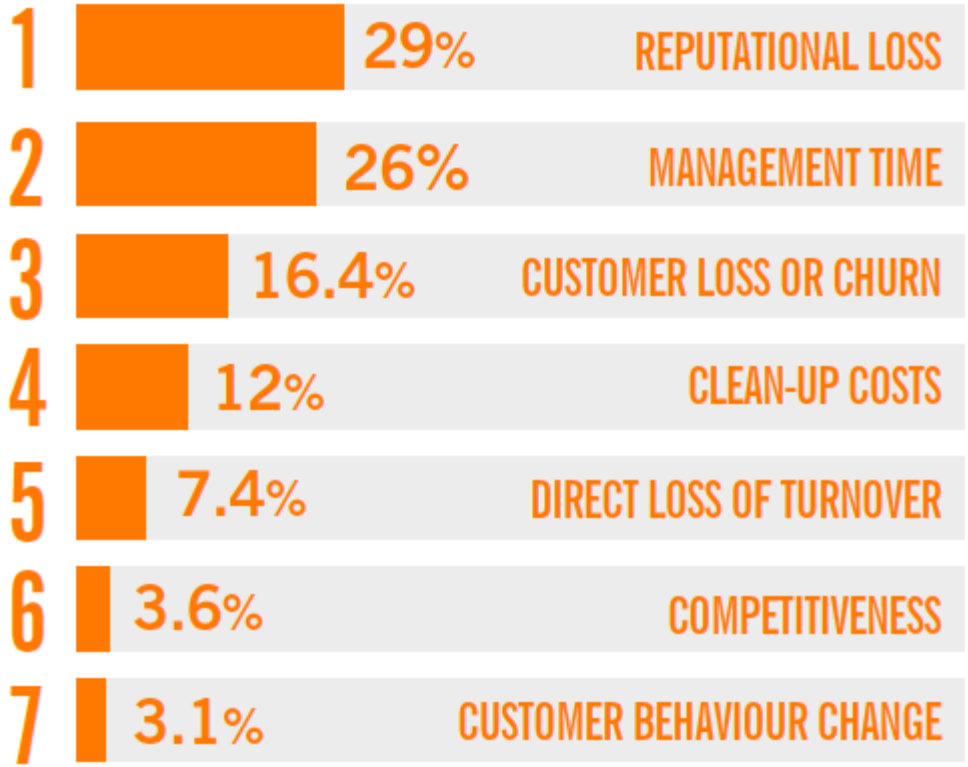
EXTORTION BY INDUSTRY



* sample size <50

Grant Thornton

WHAT IS THE PRIMARY IMPACT OF A CYBER-ATTACK?



CYBER-ATTACKS

6% INCREASE IN ATTACKS OVER THE PAST 12 MONTHS

Personal data

- name
- date of birth
- personal ID nr
- aadress
- telephone nr
- e-mail adresses
- Online identifier (such as, e-mail address, screen names, IP address, device IDs)
- Pseudonymous data

- health data, genetic data
- biometric data (fingerprint, face detection)
- disciplinary statements
- exam / test results
- other verbal assessments such as protocols for development interviews

Employee and/or client

Art 9: Special categories of personal data

- Processing of personal data revealing
  - racial or ethnic origin,
  - political opinions,
  - religious or philosophical beliefs, or
  - trade union membership,
  - genetic data, biometric data

  for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, IF….

Legal basis of processing

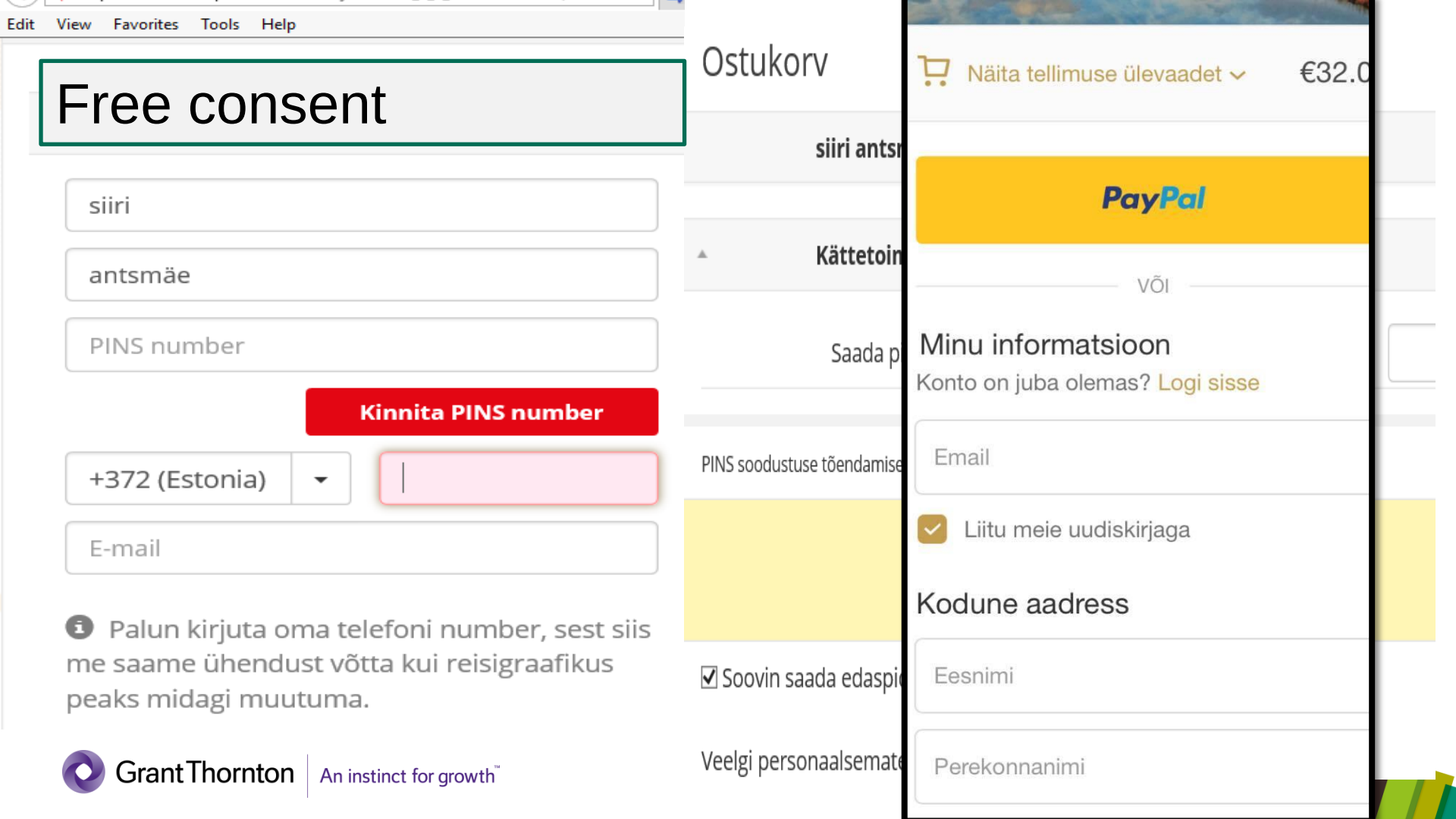
Data made public by the data subject

By law

Based on contract

Data subject's explicit consent

Specific processing situations (art 85)

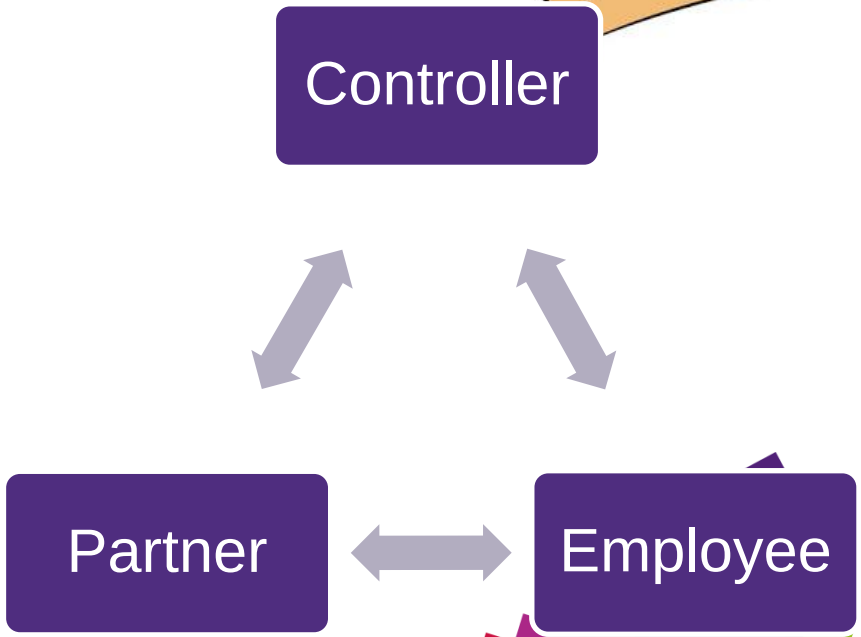

Edit View Favorites Tools Help
Free consent
siiri
antsmäe
PINS number
Kinnita PINS number
+372 (Estonia)
E-mail
Palun kirjuta oma telefoni number, sest siis me saame ühendust võtta kui reisigraafikus peaks midagi muutuma.
Grant Thornton
An instinct for growth™
Ostukorv
Näita tellimuse ülevaadet
€32.0
PayPal
VÕI
Minu informatsioon
Konto on juba olemas? Logi sisse
Email
Liitu meie uudiskirjaga
Kodune aadress
Eesnimi
Perekonnanimi

Art 5: Personal data shall be

- (a) processed **lawfully, fairly and in a transparent manner** in relation to the data subject
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is **incompatible with those purposes**;
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation**’);

Controller and processor

- Responsibility - The controller is responsible for the processor's compliance with processing principles and rules
- Controller must be able to demonstrate the compliance



Art 5: Personal data shall be

- (f) processed in a manner that ensures appropriate **security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

Access matrix

Phone mobile

Voip code

728

- [x] Saadab pakkumisi klientidele

Permissions

- [x] Vehicle registry
- [ ] Vehicle retrieval manager
- [ ] Remove from blacklist
- [ ] Unsecured reports
- [ ] Delete vehicle files
- [x] Unlock vehicle
- [ ] Vsaa
- [ ] Change status written off
- [ ] Amendment manual commission
- [x] Creditinfo ee creditscore webservice
- [ ] Debt collection entries
- [ ] Export
- [ ] For repossession reports
- [ ] Late payment collector selection
- [ ] Amendment manual conclude
- [x] Partly unlock vehicle
- [ ] Vsaa unlimited requests
- [x] Create manual payments
- [ ] Remove additional costs
- [ ] Debt hard collections
- [ ] Validation disablation
- [ ] Repossessed reports
- [x] Reporting data
- [x] Edit credit scoring fields
- [x] Manual vehicle lock
- [ ] Edit identification number
- [ ] Edit remote
- [x] Xroad rr

Responsibles set

- [x] Application
- [ ] Debtsoftcollection
- [ ] Agreement
- [ ] Invoice
- [ ] Debthardcollection

- Google Drive
- One Drive
- Azure
- Dropbox
- SharePoint
- …

The time limit for storing data is strictly limited

Kaspersky Lab report: Cybercriminals often first attempt to gain entry to an enterprise system through the weakest link: Employees

- The top concerns
  - employees sharing inappropriate data via mobile devices (47%),
  - the physical loss of mobile devices exposing their company to risk (46%),
  - the use of inappropriate IT resources by employees (44%).
- 40% of businesses globally said that employees hide IT security incidents to avoid punishment

Grant Thornton

An instinct for growth™

GROWING TOGETHER

Global strategy 2020

Self-evaluation questionnaires for organization

GDPR audit

Consulting