

# REGNSKAP NORGE



## IT-security Money laundering Hans Ellefsen, Technology and Innovation @ Regnskap Norge





П

irror\_mod.use\_x = True MIRROR\_X": irror\_mod.use\_y = False irror\_mod.use\_z = False operation == "MIRROR\_Y"; irror\_mod.use\_x = False irror\_mod.use\_y = True lrror\_mod.use\_z = False operation == "MIRROR\_Z"\* rror\_mod.use\_x = False rror\_mod.use\_y = False rror\_mod.use\_z = True

ob.select= 1 er\_ob.select=1 irror\_ob.select = 0 bpy.context.selected\_ob ata.objects[one.name].sel

int("please select exactle

-----

vpes.Operator): X mirror to the selected ect.mirror\_mirror\_x"

Wired Magazine, December 24, 2021 s. 3 30. mar. 2022

## "2021 was a year of ransomware, election at the end -add SURVeillance, data breaches, and "Selected" + str(modifie VeS, MOre ransomware"

Cryptolocker 2.0

### Your personal files are encrypted



Your files will be lost without payment on:

Your important files were encrypted on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them

Encryption was produced using unique public key RSA-4096 generated for this computer. To decrypt files, you need to obtain private key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; the server will destrov the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files.

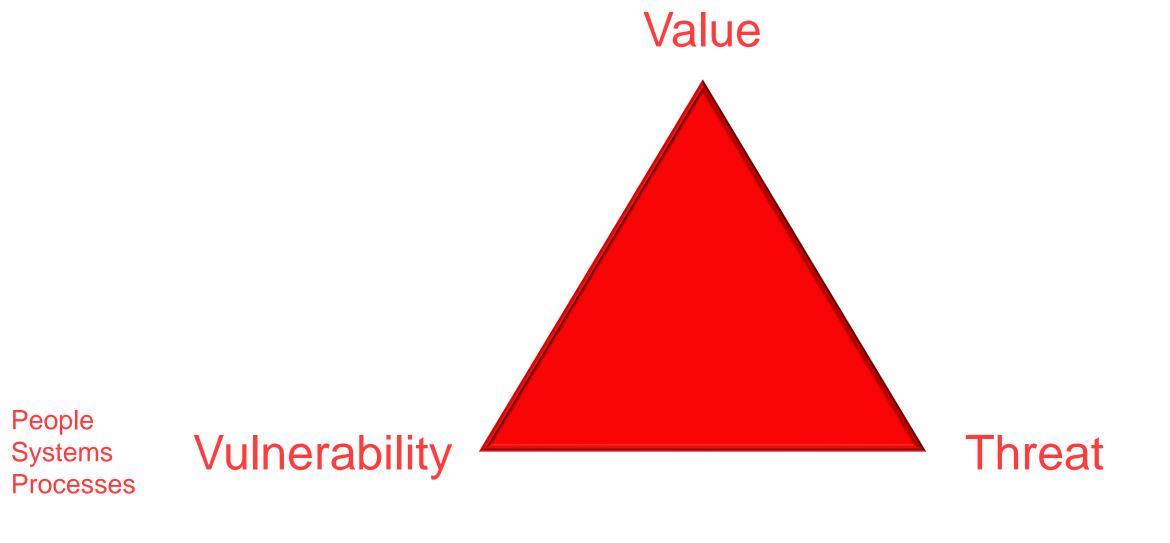
To retrieve the private key, you need to pay 0.5 bitcoins.

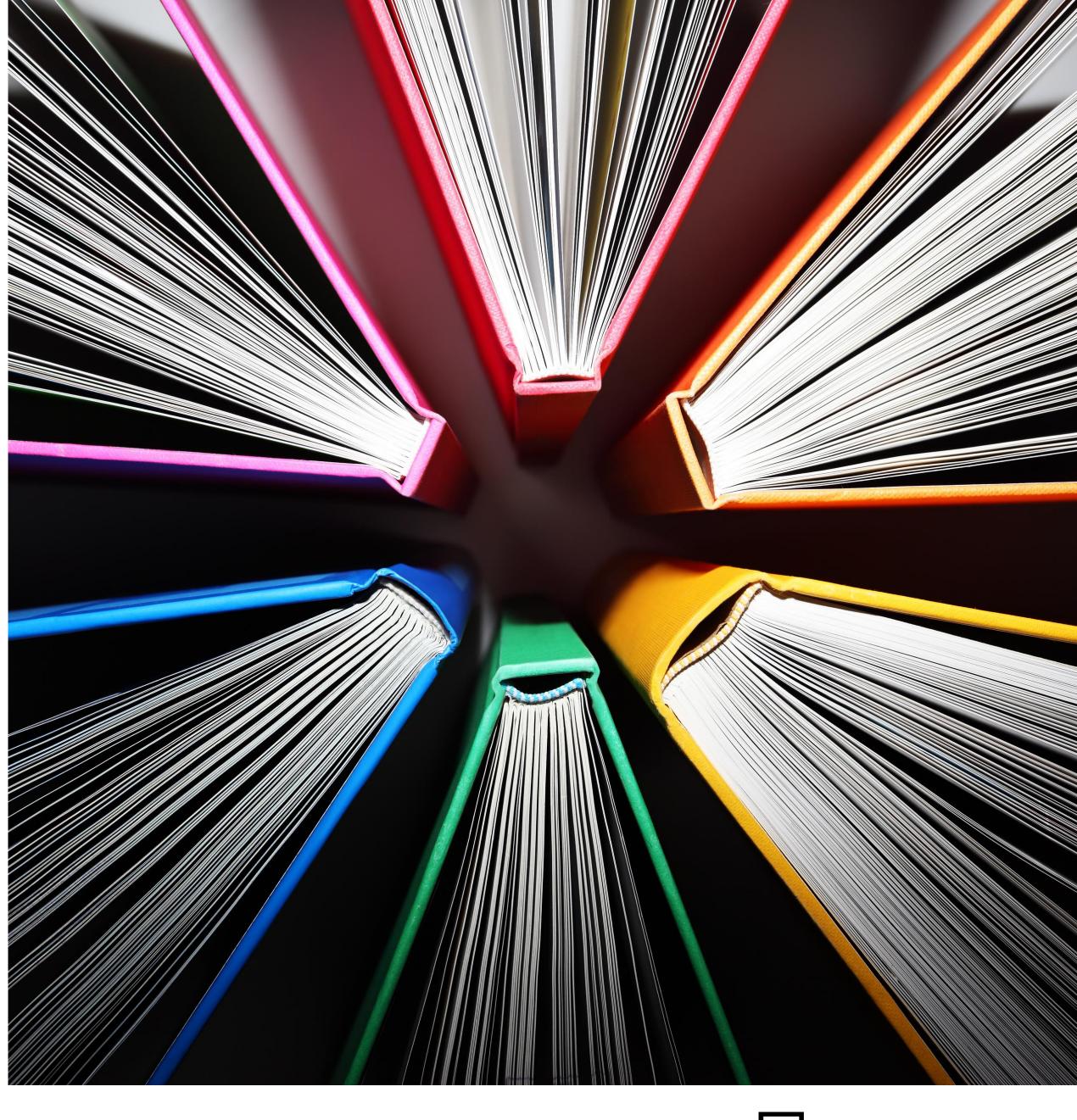




### Are the accountants at risk?

- Accounting = Handling a lot of money to steal
- Accounting = Personal information in heaps to sell
- Accounting = Company information to sell







## Top IT-security risks

- Managers do not include IT-security risk as a part of their risk analysis
  - Security as a Service not always embedded into the solutions
- Staff are not adequately aware of risks the company is exposed to
  - Phishing
  - Social Engineering
    Ransomeware

  - CEO-scams
- Loss of mobile devices
- Patches to systems are not updated on a regular basis
- Two-factor authentication is not implemented when available
- Bring Your Own Device / Software loose control
- Sensitive data in clear text Personal Data Act
- Lack of a contingency plan

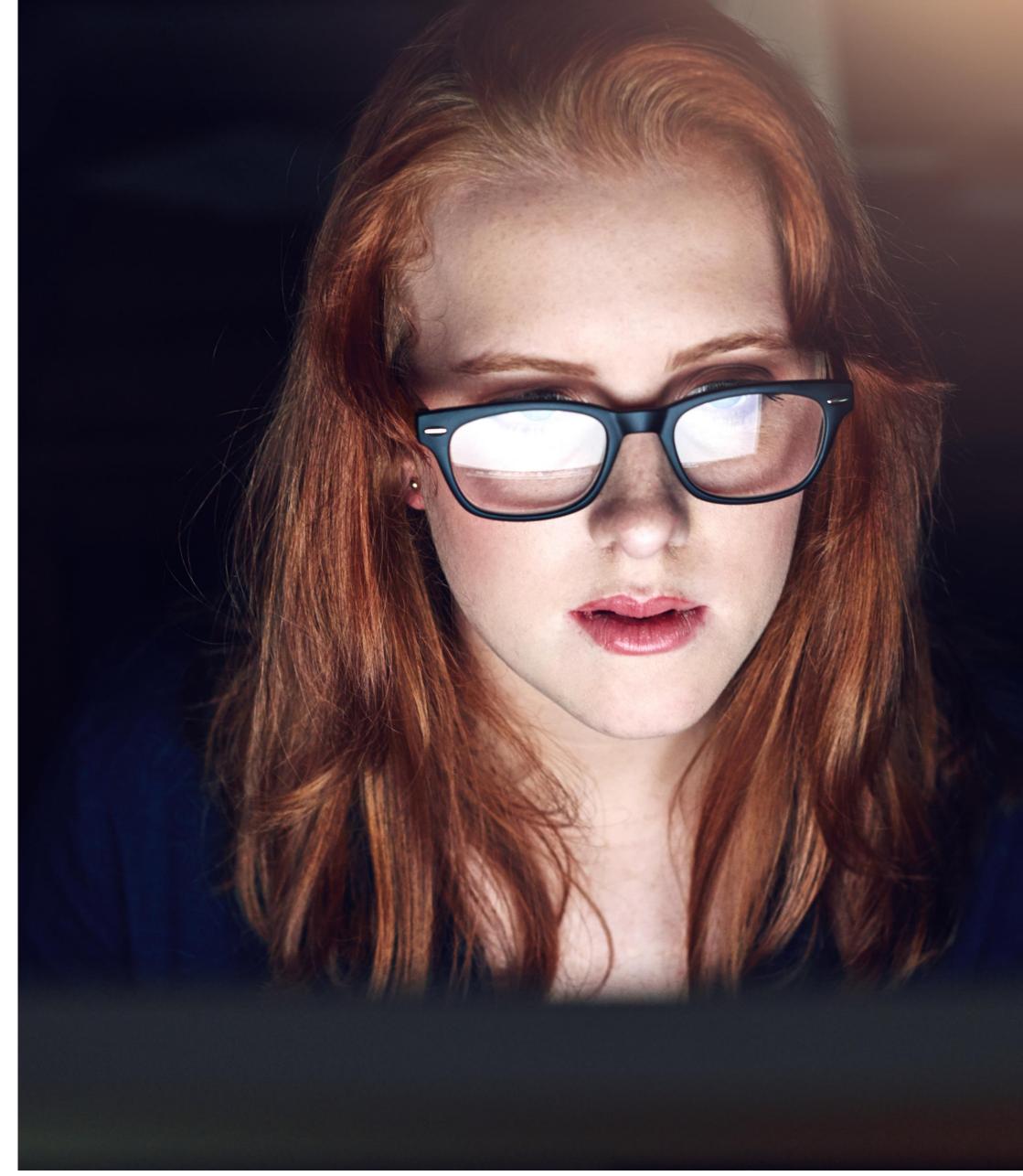






### How to be more prepared

- Risk analysis what can go wrong?
- Awareness the best tool to reduce risk
  - Training and testing staff
  - Sharing experiences
  - Learn from others
- Two-factor authentication username and password is not sufficient anymore
- Good backup routines tested contingency plans







## Money Laundering

- Proportionality between the risk at hand and the activities needed to comply with the regulation's intent
  - What is adequate?
- Expectation gap between the accountants and regulatory authorities?
  - More guidance from the authorities needed
- Too high focus on written procedures and to little attention towards the actual transactions?
  - The number of reported suspicious transactions from accountants and auditors are quite low. Why?

Country	Reported transactions from accountants	Reported transactions from auditors	Total reported transactions
Norway (2021)	104	41	16.513
Finland (2020)	31	18	61.752
Sweden (2020)	6	8	24.505







## Findings from the Norwegian Financial Supervisory Authority

- Many have used routine templates without adapting the template to their own business
- Training has probably been completed, but is poorly documented
- A risk assessment of one's own business must be carried out – where are we most vulnerable and what threats do we have to deal with?
  - In the Norwegian Supervisory Authorities assessment, this was not adequately addressed, in the sense that it did not reflect the business and there was too little writing about the assessments.
- Risk assessment of customers was also criticized
- Written explanations were missing or were deficient, and this was especially visible in cases where customers were in risk industries.
- Internal control was not sufficient. It was not adapted to the customer / identified risk.







23 35 69 00 | post@regnskapnorge.no | regnskapnorge.no

