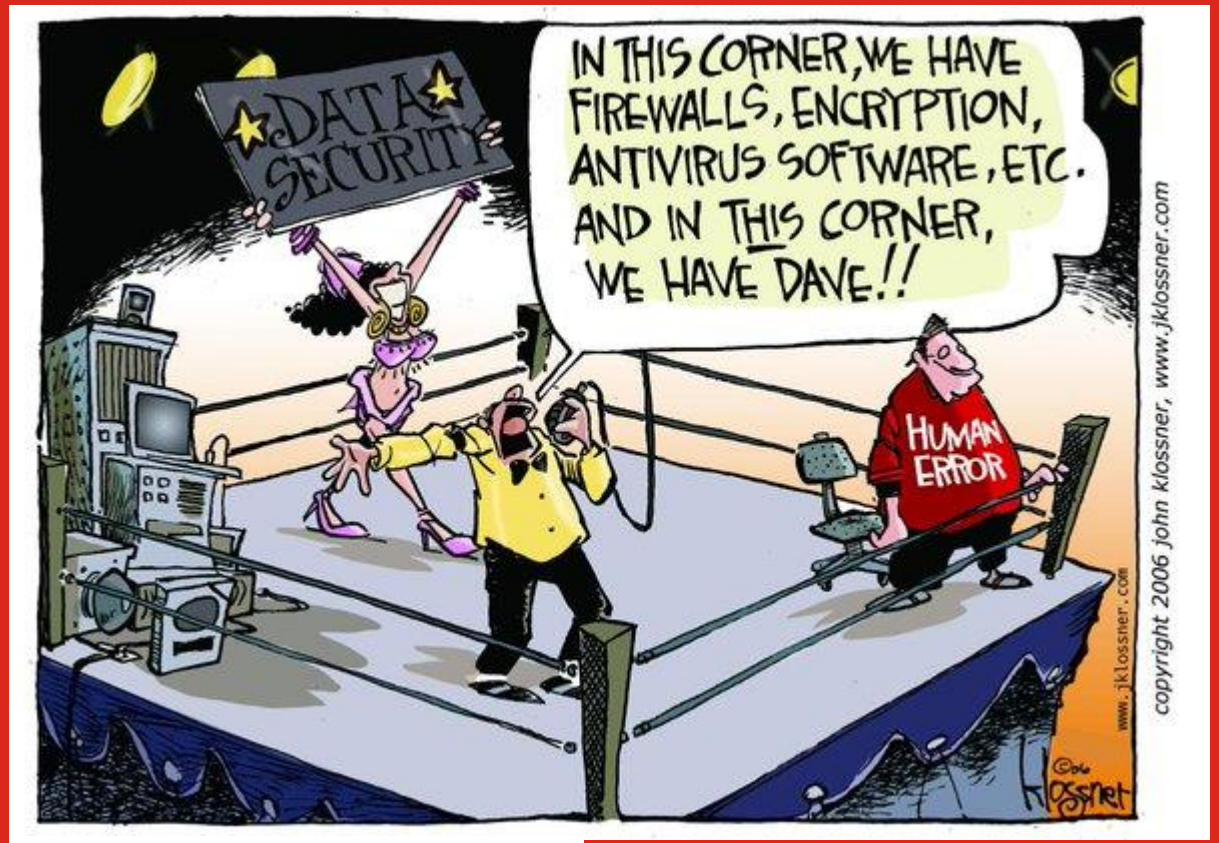
storebrand spp

ISACA
Dôvera v informačné systémy a ich prínos
Slovensko Chapter

Building security culture that *sticks*.

Bjorn Richard Watne – Chief Security Officer
CISM, CGEIT, CRISC, CISSP-ISSMP

ABIT - Conference
Bratislava, June 1st 2017



ISACA Slovensko pozýva na konferenciu Audit a bezpečnosť v IT – ABIT

About Bjorn

- BSc, Computer Science from Agder University
- MBA, Business Administration from ESCP in Paris
- CISSP-ISSMP, CRISC, CGEIT, CISM, ISO 27001 LI, ISO 27005 RM, ISO 22301 BCM, ++
- 15+ years of experience with information security
- 3 years as a Security Analyst
- 4 years as a Security Architect
- 3 years in Marketing (!)
- 4 years as a Security Consultant

ISACA®
Trust in, and value from, information systems
Norway Chapter

- Currently employed as Chief Security Officer for Storebrand.

storebrand spp

About Storebrand

Pension fund

Asset mgmt.

Insurance

Banking

Largest pension fund in the Nordics

- 40 000 business customers
- 1,9 million individuals
- £13 BN in Unit-Linked assets
- £26 BN in guaranteed assets
- 100 % managed on sustainable critereas
- Approx. 2.000 employees in Norway and Sweden

Asset management	Insurance policies	Bank, loans
£40 BN	£18 BN	£3 BN

storebrand spp

Who do we trust? (Industries)

- Technology (74%)
- Food and beverage (64%)
- Consumer goods (61%)
- Telecom (60%)
- Energy (58%)
- Pharmaceuticals (53%)
- Finance (51%)

Source: Edelman 2016. 33.000+ respondents in 28 countries

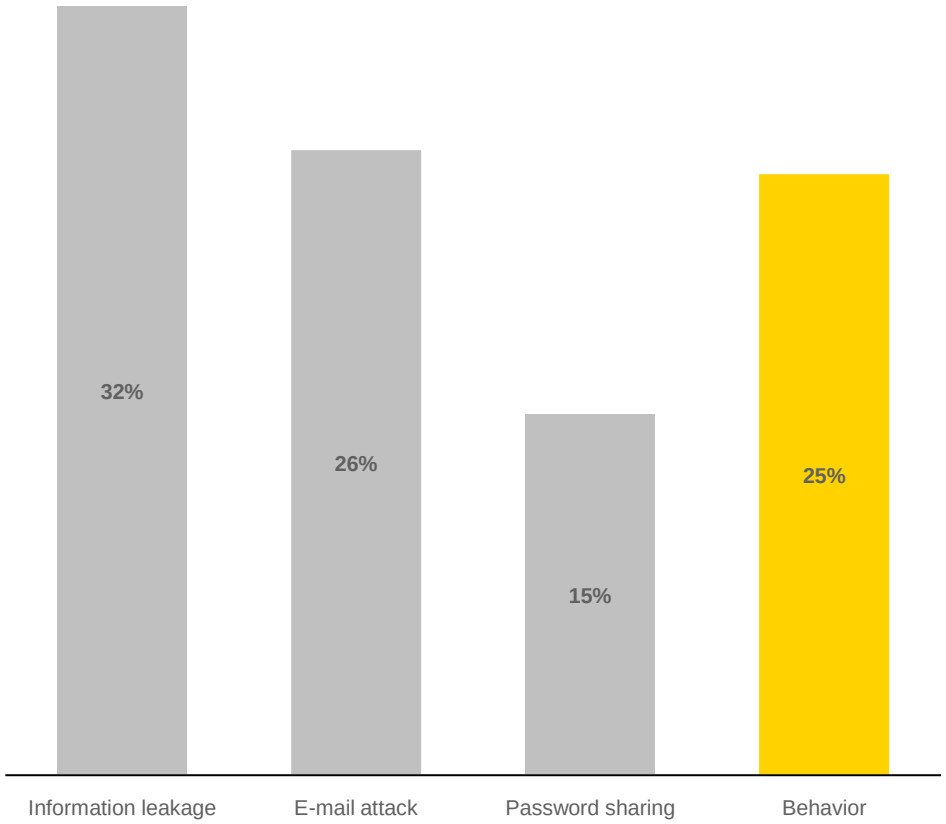
Tip #1: Aim at the top. Even the CEO has a boss.

Internal Audit performed by EY in spring 2015 to map employee awareness to information security:

"The intention was to give the board and top management, a third party assessment on employees competence, behavior and motivation on secure management of the company's information assets."

storebrand spp

Tip #2: Support the business – make a business case.



- There is a medium risk (32%) in regard to employees leaking information following external pressure.
- There is a medium risk (26%) to business systems from employees clicking malicious links in e-mails.
- There is a high risk of employees sharing their passwords (15%) thus giving an attacker direct access to business systems.
- Overall the possibility of employees conducting themselves in a way that poses a risk to the business is high.

storebrand spp

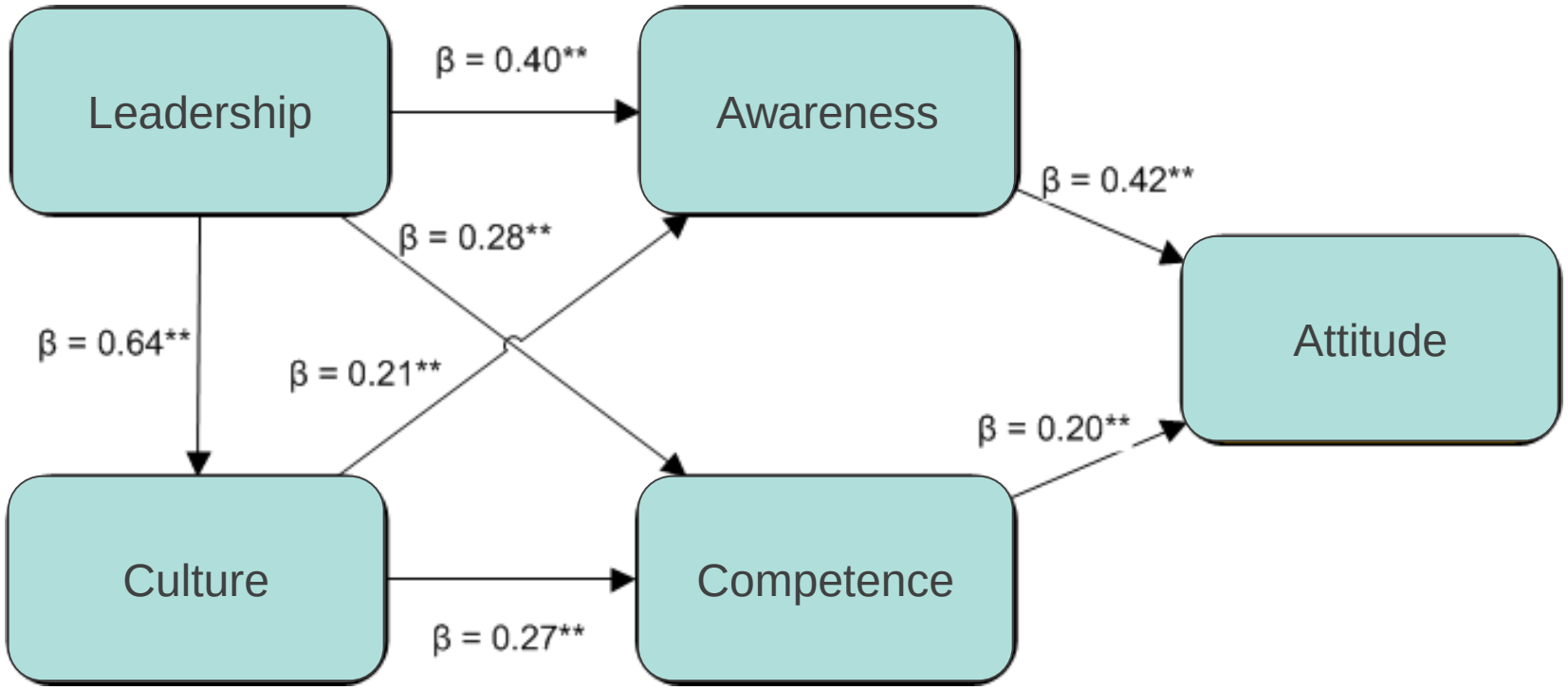
Some answers to questions about culture.

- Most employees answered "Don't know" when asked whether we have a security culture.
- Most employees answered "Don't know" when asked if they felt we have a security focused leadership.
- Only 1 in 5 employees feel they have everything under control with how to make necessary measures to protect information and IT-resources.
- Only 1 in 5 absolutely agree that managers have the ability to encourage security awareness.
- 1 in 3 agrees that information security is everyone's responsibility, and feel that colleagues are warning each other if anyone is placing themselves at risk.
- Almost 1 in 3 are confident they are competent enough to handle information and information systems in a secure way.
- Almost 2 in 5 agree they know the policy and guidelines connected to acceptable use of IT-resources, installation of software and handling sensitive information.
- 3 in 5 absolutely agree they are aware of risk and consequences of inadequate information security.
- 3 in 5 absolutely agree to information security being important, and they **like the idea of introducing necessary steps to increase it to an acceptable level.**
- Almost 4 in 5 agree to information security being necessary.

Disagree 1 2 3 4 Absolutely agree

storebrand spp

Tip #3: Pay special attention to mid-level management.

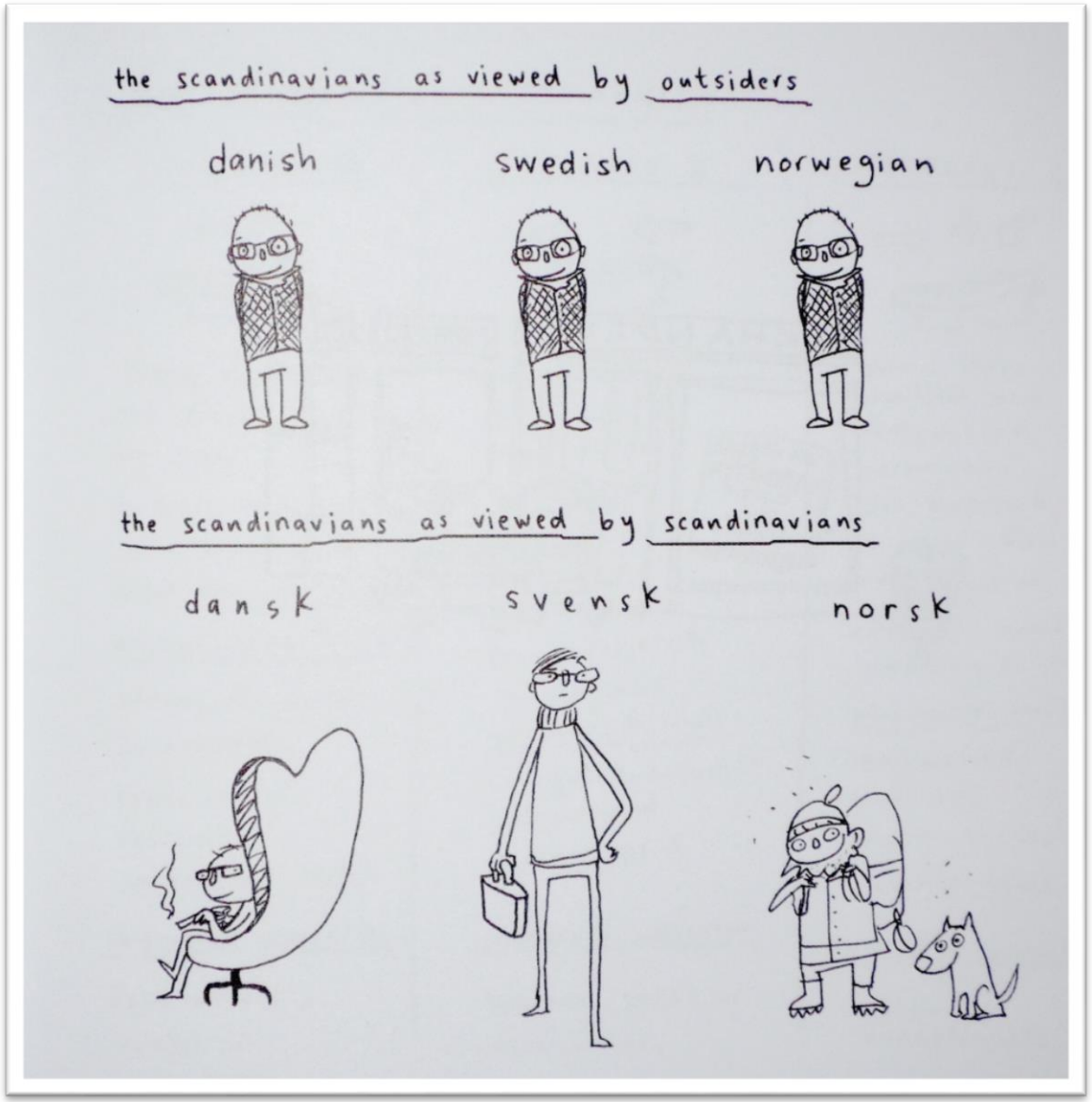


Coefficient (β)	Effect
0.1 - 0.3	Low
0.3 - 0.5	Medium
0.5 - 1.0	High

- Managers shape the employees perception on what's important and should be prioritized. The management team is what creates the employees values, and in turn the security culture of Storebrand.

storebrand spp

Tip #4: Know your audience.



Keep it interesting!

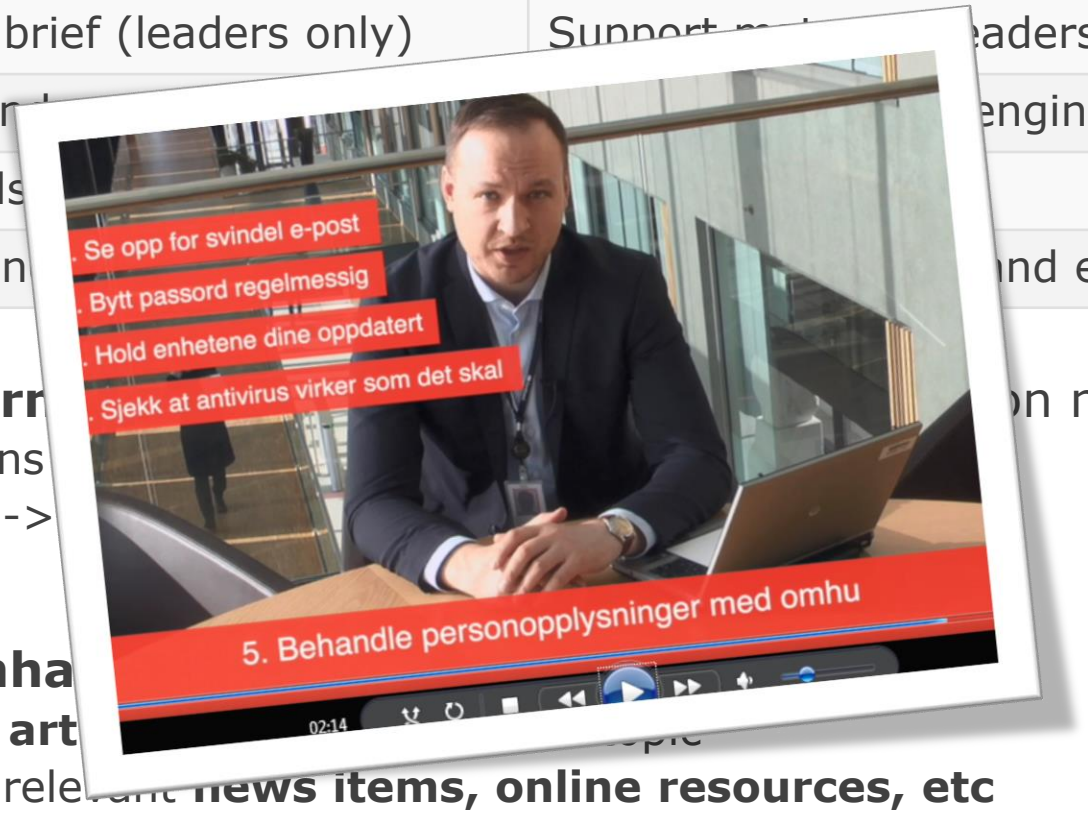
Keep it relevant!

storebrand spp

Creating "The package" – make it relevant

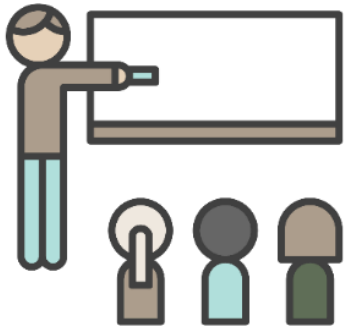
- **8 topics - 9 months**

Program brief (leaders only)	Support m… eaders only)
Threat lan…	…engineering
Passwords	
Privacy an…	…nd ends)



- **Nanolearn…** …n method
  - 17 lessons
  - Leaders ->

- Topics **enha…**
  - Intranet **art…**
  - Links to rele…vant **news items, online resources, etc**
- **Video** recorded for each topic!
- **Metrics:** Distribution–Awareness–Behaviour (sort of..)



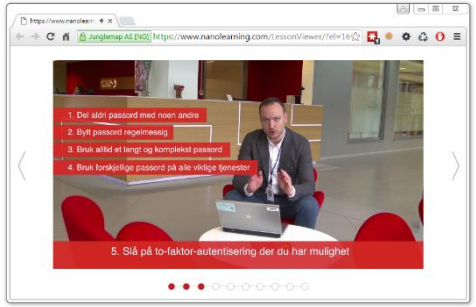
storebrand spp

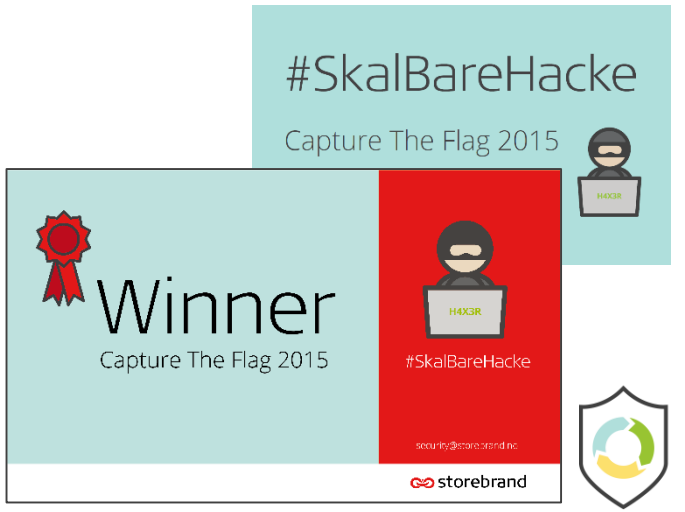
Examples > S-SDLC > Training

Training

1. Core Security Training

- Examples include
  - Storebrand/SPP Security training (Security Semester)
    - Base security awareness training
    - Core security training
    - "Hackathon" CTF
  - #SkalBareHacke
  - #SkalBareSikre





storebrand spp

About #SkalBareSikre >> Training modules

Security semester

- Basic Theory
- Basic Technical
- Heavy Technical
- Practical Assignments

"Base security awareness training (1-6 hours)"
- Storebrand/SPP policy & relevant laws
- Introduction to secure development methodology
- Security Standards

"Core security training (ethical hacking) (2-4 days)"
- HTTP & Sessions
- Introduction to Cryptography (Encryption)
- Introduction to ethical and legal "Security Testing"
- OWASP Top 10 Vulnerabilities

"Hackathon" CTF (1 day)

storebrand spp

Examples > S-SDLC > Training

Training

1. Core Security Training

- **Name:** Basic Information Security Training
- **Code:** S-SDLC400
- **Hours:** 7 Hours
- **Course Introduction:** The Storebrand/SPP Basic Information Security Training Course teaches students practical skills regarding privacy and information security.
- **Course Description:** The course includes knowledge of standards and processes to further increase the level of focus on information security and privacy. The course has the goal of teaching basic information security and privacy principles, guidelines and giving an introduction into upcoming EU GDPR (General Data Protection Regulation). Furthermore the course gives an introduction into the Secure Software Development LifeCycle (S-SDLC) and how to apply its process to development and project management activities and selected OWASP (Open Web Application Security Project) standards, such as OWASP Top 10, OWASP Testing Guide and OWASP Application Security Verification Project (ASVS), used with the S-SDLC.

storebrand spp

About #SkalBareSikre >> Training modules

Basic Theory

S-SDLC100
#Privacy, Security, laws, standards and guidelines

S-SDLC101
#Secure Development

S-SDLC102
#Security Standards

S-SDLC301
#Introduction to ethical & legal "Security Testing"

Basic Technical

S-TECH110
#HTTP & Sessions

S-TECH111
#Introduction to Cryptography (Encryption)

S-TECH210
#Introduction to Security Testing with Burp Suite

Examples > S-SDLC > Training

Training

1. Core Security Training

- **Name:** Advanced Information Security Training
- **Code:** S-SDLC600
- **Hours:** 28 Hours
- **Course Introduction:** The Storebrand/SPP Advanced Information Security Training Course teaches students practical skills regarding privacy and information security. In addition giving detailed knowledge of common web-vulnerabilities, how to find and mitigate them as well as practical hands-on testing through Capture the Flag (CTF) training.
- **Course Description:** The course includes knowledge of standards, processes, web-vulnerabilities, cryptography and security testing methodologies to further increase the level of focus on information security and privacy. The course has the goal of teaching basic information security and privacy principles, guidelines and giving an introduction into upcoming EU GDPR (General Data Protection Regulation). Furthermore the course gives an introduction into the Secure Software Development LifeCycle (S-SDLC) and how to apply its process to development and project management activities and selected OWASP (Open Web Application Security Project) standards, such as OWASP Top 10, OWASP Testing Guide and OWASP Application Security Verification Project (ASVS), used with the S-SDLC. The technical parts of the course covers the **most common web-vulnerabilities in detail**, **testing methodologies** with tools such as Burp Suite and **ethical/legal security testing practices.** The students will get to test their acquired skills in a **custom made Capture The Flag (CTF)** environment designed to mimic real world security testing.

storebrand spp

About #SkalBareSikre >> Training modules

Heavy Technical

S-RISK201
#SQL-Injection

S-RISK202
#Broken Authentication & Session Management

S-RISK203
#Cross-Site Scripting (XSS)

S-RISK204
#Insecure Direct Object Reference

S-RISK205
#Security Misconfiguration

S-RISK206
#Sensitive Data Exposure

S-RISK207
#Missing Function Level Control

S-RISK208
#Cross-Site Request Forgery (CSRF)

S-RISK209
#Using Components With Known Vulnerabilities

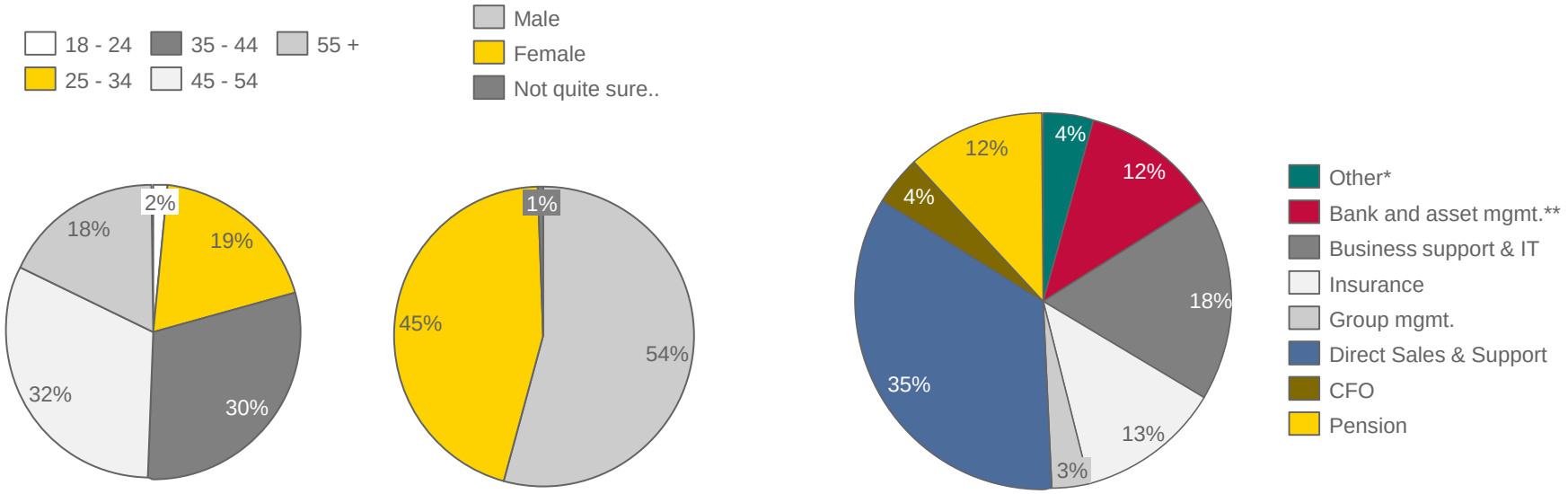
S-RISK210
#Unvalidate Redirects and Forwards

Practical assignments

S-TEST-420
#Certified Secure Capture The Flag (CTF) challenge

S-TEST-540
#Hackazon Capture The Flag (CTF) "real world" challenge

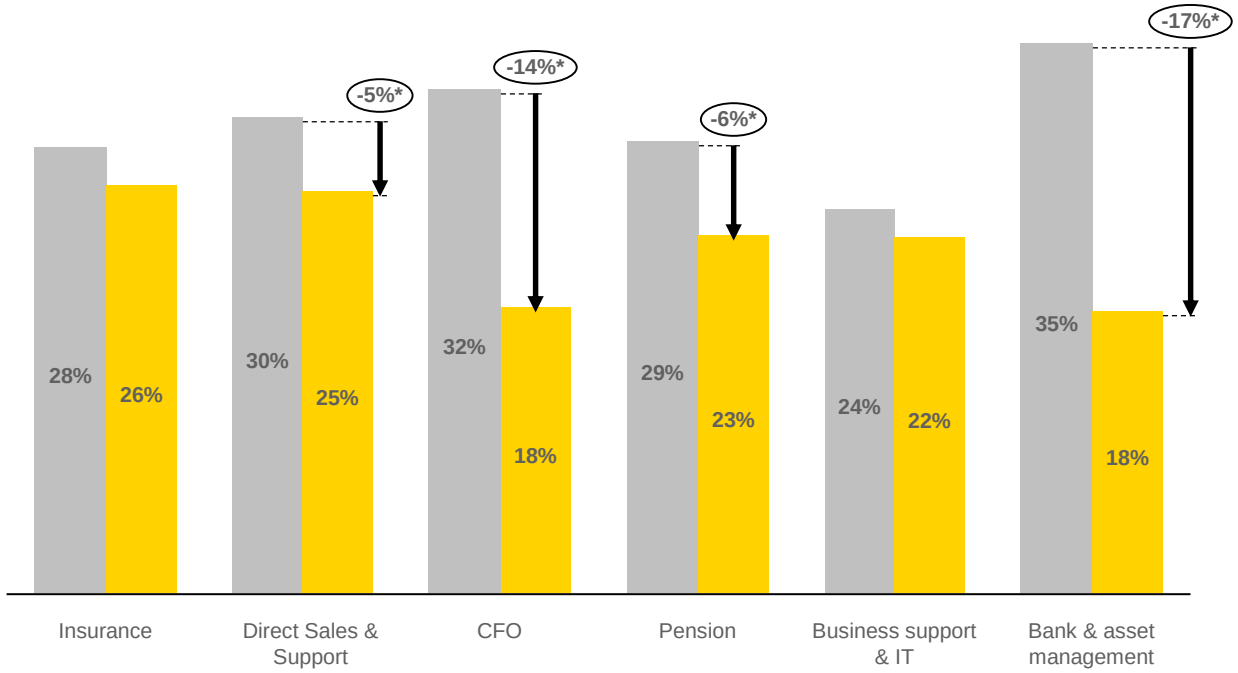
The proof is in the pudding. Back to the real world..
Employee survey: Demographic information (NO + SE)



- 1012 respondents (54 % of target group), 710 from Norway and 302 from Sweden.
- Employees aged 35-54 were the largest group among the respondents.
- Approximately 50/50 distribution of male and female respondents.

storebrand spp

Results by business areas. Norway vs. Sweden



Forretningsområde	Norway	Sweden
Insurance	83	44
Sales & Support	255	96
CFO	32	12
Pension	71	49
Business support/IT	127	52
Bank & asset mgmt.	106	11
Sum	**674**	**264**

- Employees in Norway perceive themselves more competent and aware than employees in Sweden. This is true for all the six largest business areas.
- The possibility of a successful phishing-attack is significantly higher among employees in Sweden than it is in Norway.

storebrand spp

And the winner is?

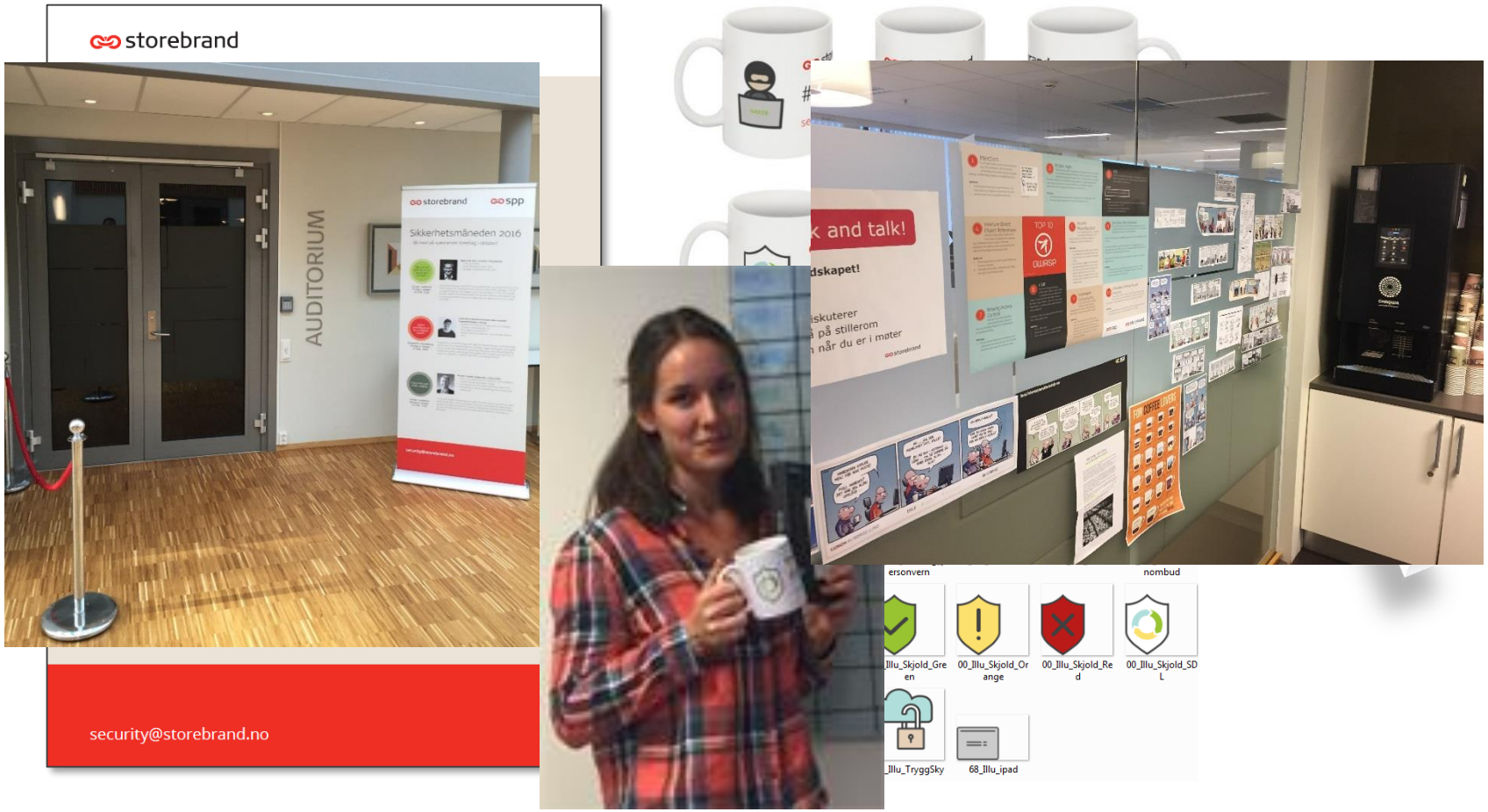
storebrand spp

Tip #5: Have fun! (even "pensioners" are competitive)

storebrand spp

Bells and whistles

Culture is a many-headed beast
- you need to attack it using every weapon in the armoury!



storebrand spp

What did we learn?

Besides Norwegians obviously feeling too good about themselves..

- **Good level of basic security awareness – but every click is one too many!**
  - Scenario was VERY easy – next one will be a lot harder
  - We didn't phish for usernames/passwords this time…
- **We need to work on incident reporting procedures!**
  - **User reports came in via 7 (!) different channels**
  - Personal emails to security crew, management, support, vendors, etc.
  - Marked difference between NO-SE-LT
- **Positive feedback from key stakeholders and users – the organization is ready**
  - TU, HR, management all backed the idea when initially proposed
  - ONE negative feedback, out of 750 recipients!

83,15% of all employees completed 100% of training

Reporting increased by 300% through right channels

More than 1.000 hours of classroom lectures given

Average rating from employees at 5/6

- **Instant wins!**
  - We're here to help: Every user that reported through correct channels got a reply thanking them for their effort
  - Procedure for reporting suspicious emails was widely communicated (replies, postings on intranet, etc)
  - The security portal on the intranet gained traction

But, does it work?

storebrand spp

Questions?

1. Aim at the top
2. Support the business
3. Mind the managers
4. Know your audience
5. Have fun!

bjorn.watne@storebrand.no

storebrand spp