Baby steps – deep footprints:

Building and launching your first security culture program

09.06.2016

Magnus Solberg, CISSP, CISM
Security Manager
Storebrand Group ASA
About Magnus

• Oslo born and raised, 80's kid
• Dad to an awesome 1-year old monster!

• CISSP, CISM, CCSK, ISO 27001 LI + A, ISO 27005 RM, ISO 22301 BCM, TLDR
  – Academic background in religious sociology/history/psychology (University of Oslo)

• 10 years in infosec proper
• First 5: Hard tech! [firewalls, emailsec, websec, mdm, idm, a/v, vpn, siem, etc]
• Last 5: Soft matter! [ISMS, CISO4hire, risk mgmt, compliance, policy, sec comms, awareness]

• Currently (and happily): Security Manager at Storebrand Group ASA

Information security begins and ends with people!
Nordic leader in occupational pension

- 40,000 corporate customers
- 1.9 million individual customers
- 128 billion NOK in Unit Linked reserves
- 266 billion NOK in guaranteed reserves
- 100% of assets managed according to sustainable criteria
- Ca. 1,900 employees in Norway/Sweden

Asset management
- 569 billion NOK in managed assets

Insurance
- 4.5 billion NOK in premiums

Banking
- 31 billion NOK in net loans

Trustworthy – Straightforward – Forward-thinking – Sustainable
Agenda

• Part 1: What we did and how we did it

• Part 2: Communicating security

• Part 3: What's next (and what's not)?
Part 1: What we did and how we did it
The mission

#SkalBareSikre: Storebrand's security culture program for the past year

- **Project mandate, iteration #1:**
  - **Primary objective:** "All employees must know what infosec *means* for Storebrand and its customers"
  - **Main target audience** – Norwegian employees (~1400 people)
    - Secondary: Swedish and Lithuanian (~900 people)
  - **Topic selection** must reflect and address findings in internal audit; obvious risks as identified by Group Security; mgmt/CRO concerns; and customers' interests
  - Program participation **NOT mandatory**
  - Lesson/topic completion goals: "Best effort"
  - Other goals, metrics, tools wholly up to us
  - **Limited budget and resources...**
(Other) challenges

• No pre-existing SC program, started on scratch

• In fact, no pre-existing Group Security department!

• Generally very brick & mortar, pre-cyber view on threats
  - Risk org. Mature (because, insurance), but no real experience with cyber risks
  - "Security" very IT focused – "not my problem"

• Incident reporting near non-existant

• Outsourcing/reorganizing -> huge changes to target groups
Step 1: Aiming for the top

- **Top management MUST spearhead the effort!**
  - Everything (yes, everything...) runs down from there

- **Lucky us:** They were on board from day 1!

- **Group CEO starred in the video intro,** urged all employees to participate.

- Other C-level suite also boosted the program to their respective verticals.

- Have shown **continuous interest** in program progress...
  - ...but of course, we also took great care to **update them frequently. 😊**
Step 2: Formulating a plan

- Need to answer WHAT – WHY – WHO – HOW – WHEN (and MORE)!

- **Baselined our entire workforce** (by hijacking our internal audit program):
  - Identified *major infosec pains* related to culture.
  - Identified *leaders* as causally significant to improving culture.
  - Combined with previous risk assessments, compliance/legal concerns, and Group Security threat knowledge, the list of topics pretty much gave itself.

- **Then:**
  - Decided to focus on only TWO *target groups*: Leaders and Employees.
  - Decided on tools, basic metrics, goals, reporting horiz/vertic, etc.
  - Selected the "hows" and "whens"
  - Put it all into a comms calendar
Step 3: Creating "The package"

- **8 topics - 9 months**
  - Program brief (leaders only)
  - Support material (leaders only)
  - Threat landscape (intro)
  - Phishing and social engineering
  - Passwords
  - Privacy
  - Video recorded for each topic!

- **Nanolearning**
  - Very cost effective
  - 17 lessons total
  - ALL tailor-made
  - Leaders got access one week in advance, incl. support materials

- Each topic enhanced with:
  - Intranet articles
  - Links to relevant news items
  - Links to online resources

- **Metrics:** Distribution – Knowledge/Awareness – Behaviour (sort of..)
Step 3 cnd.: Comms calendar
Step 4: Launch!

National Security Month is perfect!

• **4 expert speakers** in our HQ lecture hall
  ✴ Streamed/recorded sessions

• Weekly fun **infosec-quizzes** with cool prizes

• **Printed** posters, leaflets etc

• Visited **department meetings** and other forums

• Used every opportunity to **market** the upcoming security awareness program

• **Several hundred attendees** on lectures

• **Same on quizzes**

• Leaders committed to the program

• "**Everyone**" suddenly knew about the Sec Dept.
The devil's in the details

• Built a brand new **Security Portal** from scratch – THE go-to place for "everything security"

• Ran **phishing assessments** on each geographical area

• Improved our **ISMS** immensely – policies, procedures, technical controls

• Worked hard on **security communications** – more on that in a bit
Step 6: Adding the bells and whistles

- **Culture is a many-headed beast - you need to attack it using every weapon in the armoury.**
Sidestep: Don't forget the experts...

- Special track for developers – SDLC!
- OWASP top 10
- Classroom lectures
- Mix of theory and hands-on exercises
- Hackathons with awesome loot!

### 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
Results

• Main win: Top mgmt are very happy – the program lives on!

• Quantitatives:
  • Completion rate for each lesson: Average 80%! (~1100 employees)
  • Average topic score (1-6): 4.9!
  • Incident reporting: Up 300% (good or bad?)
  • Visits on Security Portal: Average 200/month
    - "News items" on front page far more

• Qualitatives:
  • Actually being asked to participate in (nearly) all Group projects, processes, initiatives
  • Avoided several huge threats (phishing, vishing, network/system vulns, CEO-fraud, cryptovirus, etc)
  • Getting LOTS of love from employees and leaders alike – people actually WANT to learn, be safe, be productive!

GREAT SUCCESS
Part 2: Communicating security
No (wo)man is an island

• There is **no way** you can pull this off all by yourself.

• Infosec professionals ≠ people persons (?)

• Building a positive security culture is **all about working together**.

• We need to join forces with those who have **authority, tools, know-how, and vested interests**…
  - Privacy, compliance, legal
  - HR
  - Marketing
  - Dept. leads
  - Employee "alphas"

• **Find a professional partner!**
Knowing your audience

• **What you say is as important as how you say it**

• We're lucky: **Storebrand org culture is awesome** – and employees *are* conscious of their responsibility (*but* awareness/knowledge/conduct varies)

• Few target groups = **both easy and difficult**.

• Our demographic:
  - **Heterogenous** (age, gender, specific work area)
  - **Homogenous** (cultural/geographical background, industry sector)

• **Main learning material**: Easy-to-grasp – without insulting their intelligence
  - Saved "hard" stuff for specific audiences
  - Presentations, meeting participation, articles/whitepapers, and 1-to-1 comms.

• **No-one's "just" an employee.**

• Learning material should also cover **stuff they need at home**.

• **Showing that you care** about them and their families goes a long way to motivate **continuous participation**!
Communicating security to the top

• Top level management are clever and busy people
  – Adapt your message

• Security is a business enabler, not a show-stopper

• C-level must receive special attention due to their company-critical functions.
  – Memorandums (e.g. CEO-fraud), info on specific, relevant security concerns (e.g. outsourcing), etc

• Worst case: Use compliance and risk as motivators
  – But avoid FUD

• Report success, but don't over-report
It's all about communication

• **How much is too much?**
  - Lecture reminders, reports, "happenings", other comms

• What's the best way to convey a security message?

• All team members need to work on **"positive security communication"**
  - From "department of no" to "department of GO!")
  - Working consciously on **striking up convos**, attending dept. meetings, scratching people's backs

• Increased focus on **incident reporting** also means **responding quickly** and being **grateful** for the extra work!
Tangibles/artifacts/environment

Results

<table>
<thead>
<tr>
<th>Rank</th>
<th>Nick</th>
<th>Name</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Geir</td>
<td>(Winner CTF 2015)</td>
<td>70141 Points</td>
</tr>
<tr>
<td>2</td>
<td>0x4E71</td>
<td></td>
<td>33176 Points</td>
</tr>
<tr>
<td>3</td>
<td>Cmartin</td>
<td></td>
<td>10389 Points</td>
</tr>
<tr>
<td>4</td>
<td>t-boss</td>
<td></td>
<td>9503 Points</td>
</tr>
<tr>
<td>5</td>
<td>CaptainCrunch</td>
<td></td>
<td>8507 Points</td>
</tr>
<tr>
<td>6</td>
<td>ServeAce</td>
<td></td>
<td>8083 Points</td>
</tr>
<tr>
<td>7</td>
<td>Kai</td>
<td></td>
<td>7695 Points</td>
</tr>
<tr>
<td>8</td>
<td>1038Moss</td>
<td></td>
<td>6530 Points</td>
</tr>
<tr>
<td>9</td>
<td>Peccator</td>
<td></td>
<td>5826 Points</td>
</tr>
<tr>
<td>10</td>
<td>CozmoKramer</td>
<td></td>
<td>4885 Points</td>
</tr>
</tbody>
</table>
### Sikkerhetsportalen

**Ansvarlig:** Magnus Rønnes Solberg  
**Sist endret:** 24.10.2016 11:43:12

<table>
<thead>
<tr>
<th>Personvern på 1, 2, 3</th>
<th>Sikkerhetsportalen</th>
<th>Tips på kollega om denne siden</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapporter en hendelse</td>
<td>Ofte stille spørsmål</td>
<td></td>
</tr>
<tr>
<td>Hvis du blir truet</td>
<td>Nå du lærer på omkring sikkerhet i Storebrand? Se her først!</td>
<td></td>
</tr>
<tr>
<td>Regler og rammeverk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eLæring og kurs om sikkerhet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fysisk sikting, adgangskontroll, brann og EMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reisetot og hjemebane</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Konsernsikkerhet i Storebrand</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ofte stille spørsmål</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sikkerhetsmåned</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slutteressurser for ledere</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Nyttige lenker

- Rekkefølger for informasjons sikkerhet i konsernet
- Siste artikler fra Konsernsikkerhet
  - Den store sikkerhets-quiz: Runde 3
  - Virksomhetssikkerhet fra Microsoft
  - Den store sikkerhets-quiz: Runde 2
  - Social ingenjørskompetanse - Varfor användaren är den svagaste länken
  - Den store sikkerhets-quiz: Runde 1
  - Vårenom til Sikkerhetsmåneden
  - Vårenom til Sikkerhetsmånaden 2016
  - Kartlegging av sikkerhetskultur
  - Ny bøger med virus-e-post
  - Mail med virus til mange ansatte
  - Svindelforsøk mot Storebrand
  - LinkedIn-passord
  - Twanger kryptering av e-post
  - Ny datakyndighetsordning
  - Advarsel: Nettic-e-poster fører til virus
  - Joachim Klasson ny informationssikkerhetsoffiser
  - Falske LinkedIn-profiler brukes til svindel
  - Store mengder farlige e-poster
  - Sterk sikring i selskapets telefoner
  - Sikkerhetsbrev fra London
  - eFalsk - Phishing-angrep mot Storebrand-ansatte
  - Sikkermakuer: Vinner av hovedprisen
  - Kartlegging av ansatte - vær på vakt
  - Farlige e-poster fra Post Nord og Posten
  - Vellyktet start på Sikkerhetsmåned
  - Farglig virus harer i LDL - Storebrand også utsatt
  - Sikkerhets-Norge interessent i Storebrand
  - Falsk e-post fra Posten lenker til FARPUG VIRUS
  - LastPass hacket - Forandre masterpasswordet ditt!
  - Phishing-test viser gode resultater
  - Bonus: Phishing-mallene (med tips til hva du bør se eller)
  - Informasjonssikkhet i ferien
  - Vellyktet sikkerhetsarrangement på Lysaker
  - Phishing-angrep mot svenske brukere

---

Er det noe du savner på disse sidene, har du spørsmål, sikkerhetsIPS, eller innspill til forbedringer? Send oss gjerne en e-post på security@storebrand.no

---

![Storebrand Logo](storebrand.png)
Part 3: What's next (and what's not)?
Some lessons learned...

- **Tried to do too much, too fast**
  - You're probably more mature than your organization

- **Culture can be radically different** only an hour's flight away
  - No such thing as a "Nordic culture"

- **Too little tie-in** with other corp skillbuilding initiatives
  - Fight the noise!

- **Begging for forgiveness instead of asking for permission doesn't always work**
  - Feet were stepped on

- **Wasted** a good bit of money
  - When the perfect becomes the enemy of the good

- **Should have responded more quickly** to feedback
  - Practice what you preach
Where do we go from here?

Next iteration of #SkalBareSikre launches Jan/Feb 2017

• **Goals:**
  - Officially adding Sweden to the fold
  - Granulated target groups (more individual learning paths)
  - Optimized learning materials
  - Improved metrics

• **Preparations:**
  - New partner, specializing on security culture
  - Just sent out a new baseline survey, company-wide
  - Translated all nano modules to Swedish, closed captioned all vids
  - Launched them all at once – "spray & pray"

• **Meanwhile:**
  - Just finished National Security Month 2016, great success!
  - Publishing articles, alerting on security concerns, refining incident response
  - Working "in-line" to keep security top-of-mind
Thanks! Questions?