# eHEALTH TRENDBAROMETER

HIMSS Analytics

Results, 3rd Quarter 2016

## "Cybersecurity"

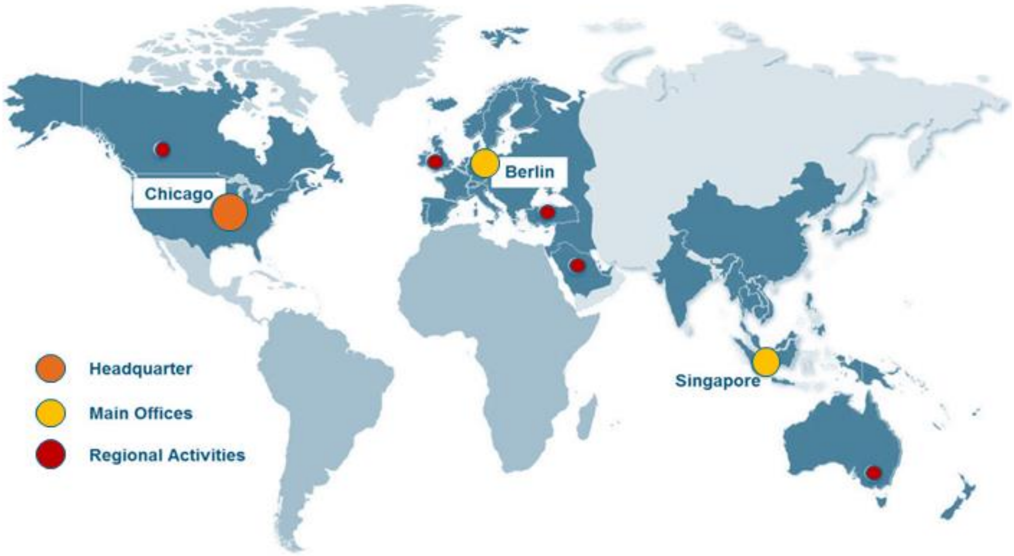
# TABLE OF CONTENT

- Results

# HIMSS ANALYTICS – WHO WE ARE

- HIMSS Analytics in Europe provides healthcare organisations, governments and industry with extensive data resources and services about the adoption and use of healthcare IT in Europe. HIMSS Analytics’ offerings include database and advisory solutions which encompass market research, IT adoption benchmarking, IT Maturity Models for topics like Electronic Medical Records or Continuity of Care. These offerings are designed to support Management and CIOs, IT Executives and Clinicians from across Europe to compare and measure their progress.

- Services categories:
  - Maturity models
  - Research & Evaluations
  - Market data



# SURVEY OVERVIEW
# GENERAL

- Objectives
  - Evaluation of trends and issues in the European eHealth sector
  - Insights into current and desired states of eHealth in Europe
  - Discussion impulses for the European eHealth community
- Study design
  - Structured qualitative online survey
  - Participation via personal e-mail invitation – European eHealth community
  - Participation via shared public link on several HIMSS media channels
- Survey period
  - 11 July – 31 August 2016
- Target groups
  - Employees in health facilities (e.g. Physicians, CIO’s, CEO’s, Nurses)
  - Employees in the eHealth related academic sector (e.g. Lecturer)
  - Employees in various eHealth related organisations (e.g. Industry representatives)

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016

# SURVEY OVERVIEW QUESTIONS “CYBERSECURITY”

1. Are you working in a health facility?
2. Has your organisation been attacked by cybercriminals over past 12 months?
3. Are you regularly updated by your organisation regarding current IT security threats?
4. Does your organisation have a business continuity plan in place to respond a cyber-attack?
5. If hackers encrypted confidential data from your organisation, would your organisation pay the ransom to get the data decoded?
6. If hackers encrypted confidential data from a care provider organisation, do you think they would pay the ransom to get the data decoded?
7. What do you think is the weakest spot for your organisation in terms of cyber-attacks?

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016

# SURVEY OVERVIEW
# QUESTIONS “CYBERSECURITY”

8. What do you think is the weakest spot for care provider organisations in terms of cyber-attacks?

9. In terms of IT environment in your organisation:
   What is the greatest area of vulnerability for attacks?

10. In terms of IT environment in a care provider organisation:
    What is the greatest area of vulnerability for attacks?

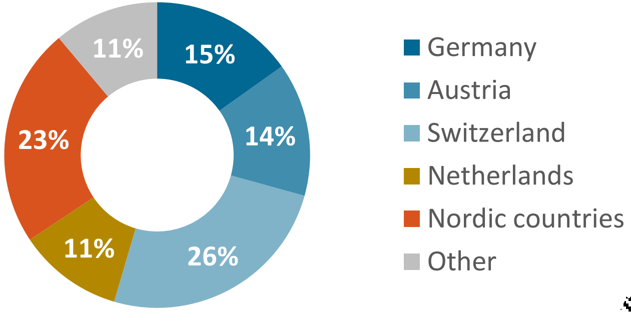
11. In your individual role as a patient:
    Is your personal health information adequately protected by health care providers in your country?

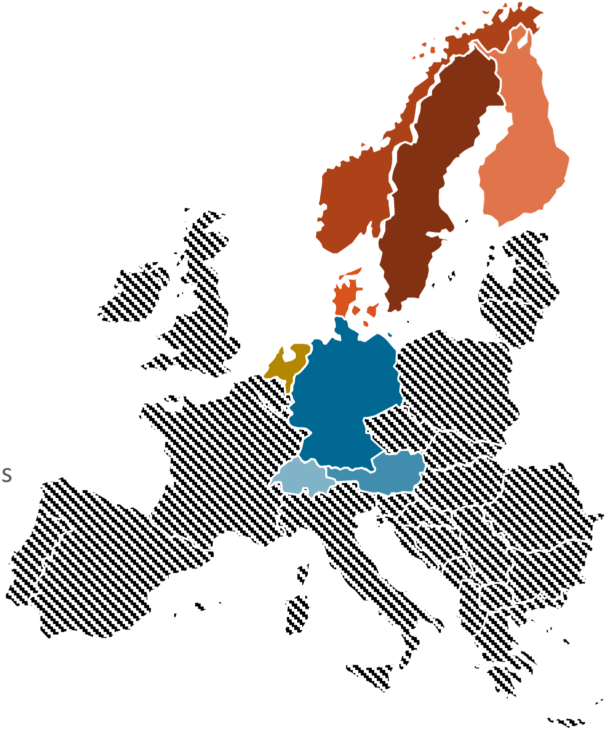
12. How will the environment for eHealth innovation and investment in your country develop over the next 12 months?

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016

# SURVEY OVERVIEW DEMOGRAPHICS

High participation from D-A-CH region and the Netherlands.
“Nordics” (i.e. Denmark, Finland, Norway and Sweden) also participated actively.



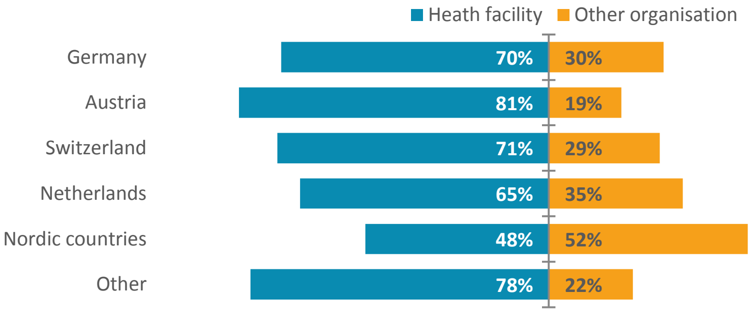


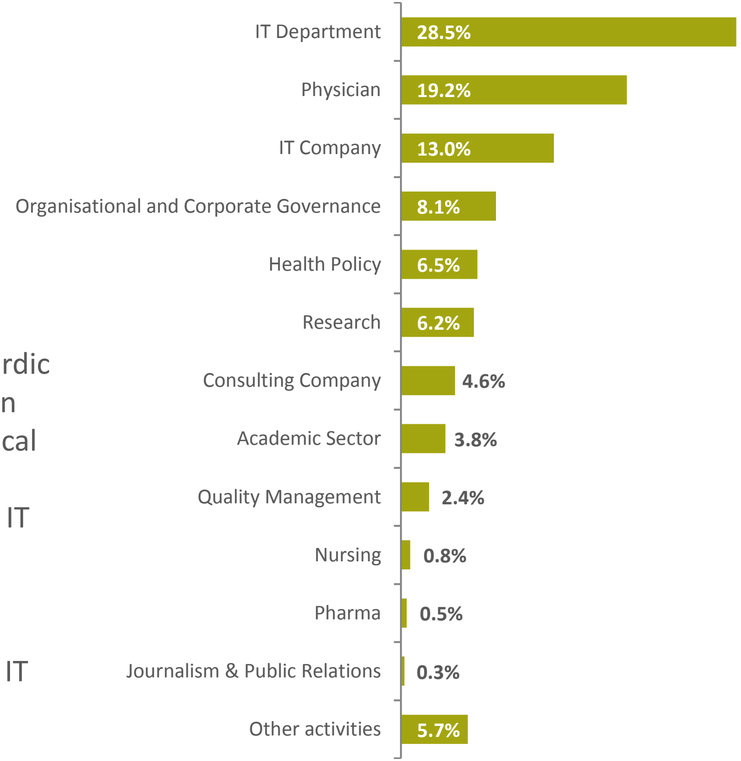
| Country | n |
|---|---|
| Austria | 54 |
| Germany | 56 |
| Switzerland | 94 |
| Netherlands | 43 |
| Denmark | 27 |
| Finland | 16 |
| Norway | 28 |
| Sweden | 15 |
| Other | 41 |
| **Total** | **374** |

“Other” comprises respondents from United Kingdom, Poland, Russia, Turkey and more.

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; Total sample: n=374

# SURVEY OVERVIEW
# PARTICIPANTS' OCCUPATION





The majority of participants work in a health facility. Only in the Nordic countries the participation from "other organisations" is higher than those from health facilities. Health facilities include hospitals, medical practice and medical care centres.

Respondents working for "other organisations" are employed in an IT Company (13.0%) or in health policy (6.5%), as those are exclusive categories regarding not working in a health facility. 5.7% of the respondents stated other activities as the listed ones.

Most of the respondents employed in a health facility are from the IT Department (28.5%) or work as physicians (19.2%) as those are exclusive categories regarding the work in a health facility.

Source: HIMSS Analytics; Study „eHealth trend barometer"; Survey period July to August 2016; Valid cases for type of organisation working for: n=374; Germany: n=56; Austria: n=54; Switzerland: n=94; Netherlands: n=43; Nordic countries: n=86; Other: n=41; Valid cases for job categories: n=369 without "Unknown job category"

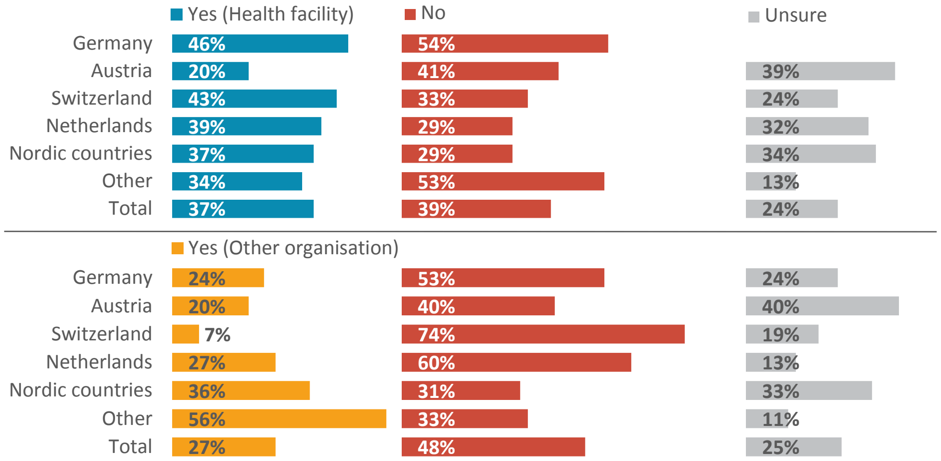
# OVERALL RESULTS
# CYBERSECURITY IN EUROPE

- Cybercrime is real: One third of employees from health facilities reported that their organization was attacked by cybercriminals during the last 12 months. In Germany almost every second one.
- Most employees are aware about current IT security threats. However, one in three employees from German health facilities do not feel adequately updated about current IT security threats.
- A majority of health organisations claim to have a business continuity plan in place, in the event of an attack. In Germany, where most of the attacks were witnessed, about one in four organisations do not have such a plan.
- Some organisations would pay a ransom to cybercriminals in order to get data decoded. About half of the surveyed health facilities would surely exclude that option.
- Human errors are the most risky factor for data security in a health facility.
- Email is perceived to be the area of greatest vulnerability for cyber attacks.
- The perception of data security varies strongly across Europe. Respondents from the Nordic countries feel relatively safe about their patient data (84% see their data adequately protected). In Germany this perception is much lower (48%).

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016

# RESULTS – CYBER ATTACKS

## 2. Has your organisation been attacked by cybercriminals over past 12 months?



### Cyber crime is a reality.

A total of 37% from all respondents working in a health facility stated that their organisation had been attacked by cybercriminals during 2015/2016.

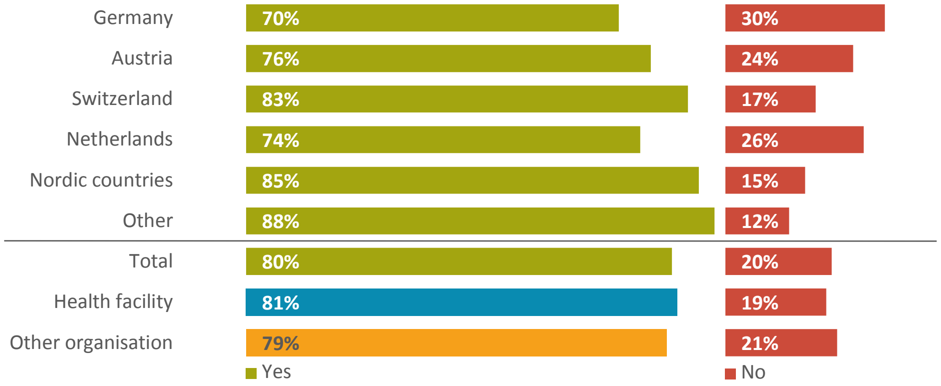
Germany seems to be one of the prime targets for healthcare-related cyber attacks in Europe. Almost every second respondent working in a health facility in Germany ("Yes": 46%) stated that they had been attacked by cybercriminals within the last 12 months.

A considerable share of professionals is not well aware about actual cyber attacks in their organisation. This is especially true for Austria and the Nordic countries where more than 1 in 3 respondents are unaware of such attempts.
Almost three-quarter of respondents from Switzerland not working for a health facility stated that their organisation not had been attacked during the last year by cybercriminals ("No": 74%). For Germany every second respondent working in a health facility gave the same answer for their organisation ("No": 54%).

Source: HIMSS Analytics; Study „eHealth trend barometer"; Survey period July to August 2016; Valid cases for working in a health facility: n=251 (Germany: n=39; Austria: n=44; Switzerland: n=67; Netherlands: n=28; Nordic countries: n=41; Other: n=32); Valid cases for working in a other organisation facility: n=123 (Germany: n=17; Austria: n=10; Switzerland: n=27; Netherlands: n=15; Nordic countries: n=45; Other: n=9)

# RESULTS – AWARENESS

## 3. Are you regularly updated by your organisation regarding current IT security threats?



Overall 80% of eHealth professionals receive regular updates on IT security threats, i.e. their organisations seek to improve awareness.

On the other hand 1 in 5 professionals have a perceived knowledge gap in that aspect. Given that it typically only needs 1 leak to enter a fortress, there seems to exist opportunities for improvement.

Respondents from the Nordic countries stated most often to receive updates by their organisations regarding current IT security threats (“Yes”: 85%).

Germany with the highest cybercrime attack rate from all countries surveyed (see slide 10) seems to have the lowest employee awareness with regards to current IT security threats (Germany “No”: 30%). This is 10% higher than the average from all survey respondents (Total “No”: 20%).

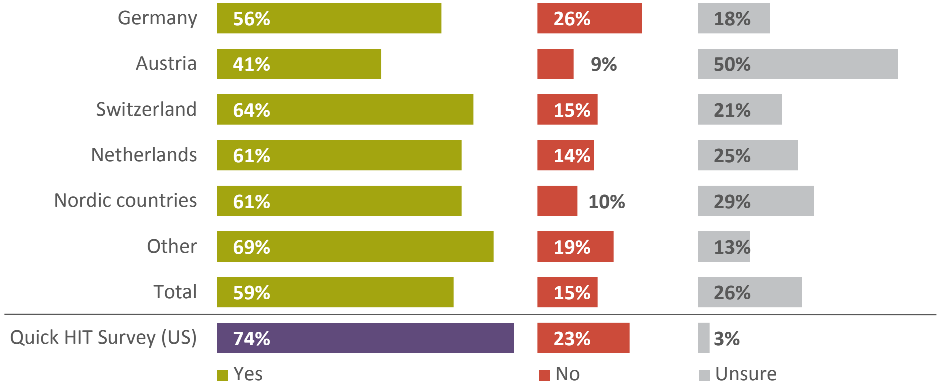
*Side note: The survey did not reveal relevant differences between respondents from health facilities and non-health facilities.*

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; without “Don’t know”; Germany: n=56; Austria: n=50; Switzerland: n=93; Netherlands: n=43; Nordic countries: n=81; Other: n=41; Total: n=364; Valid cases for working in a health facility: n=242; Valid cases for working in a other organisation facility: n=122

# RESULTS – BUSINESS CONTINUITY

## 4. Does your organisation have a business continuity plan in place to respond a cyber-attack?

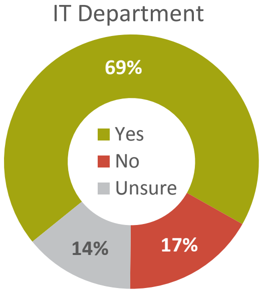
[only participants who are working in a health facility]



59% percent of all respondents working in a health facility said that their organisation have a business continuity plan in place, in the event of an attack (Total “Yes”: 59%). About 26% could not confirm if their organisation have a plan or not (Total „Unsure“: 26%).

Again, German health facilities seem less well prepared than those from other countries (26% have no such plan).

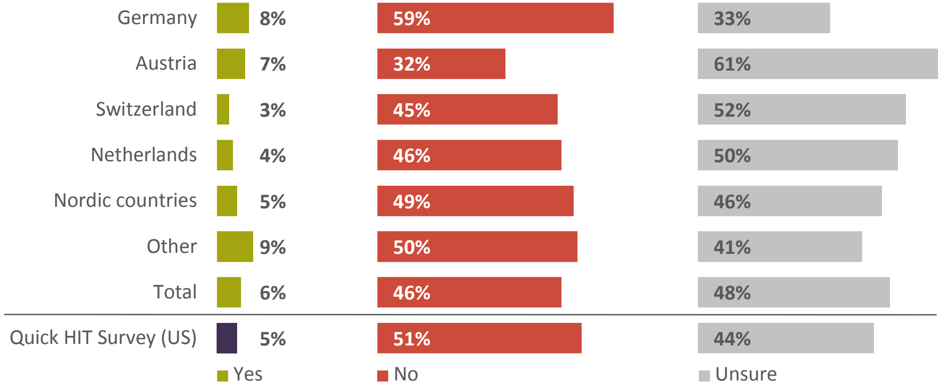
Research in the United States of America (HIMSS Analytics Quick HIT Survey: Ransomware) has shown that seventy three percent of the health systems there had a business continuity plan in place to respond a cyber-attack (“Yes”: 74%). This is slightly higher than the European average (“Yes”: 59%).
Looking only at surveyed IT staff from health facilities (see pie chart), shows in essence that both sides of the Atlantic are not far apart in the aspect of being prepared (IT Department “Yes”: 69%).



Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; only employed in a health facility; Germany: n=39; Austria: n=44; Switzerland: n=67; Netherlands: n=28; Nordic countries: n= 41; Other: n=32; Total: n=251; IT Department: n=105; Quick HIT Survey (US): www.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months refers to US hospitals

# RESULTS – PAYMENT OF RANSOM

## 5. If hackers encrypted confidential data from your organisation, would your organisation pay the ransom to get the data decoded? [only participants who are working in a health facility]



When asked if their organisation (health facility) would pay the ransom, almost half of respondents said they are “unsure” (48%). A little less are relatively sure that no money would be paid.

Interestingly, 6% of European respondents think that their organization would pay a fee to cyber criminals.
Is this the opportunity cyber criminals are looking for?

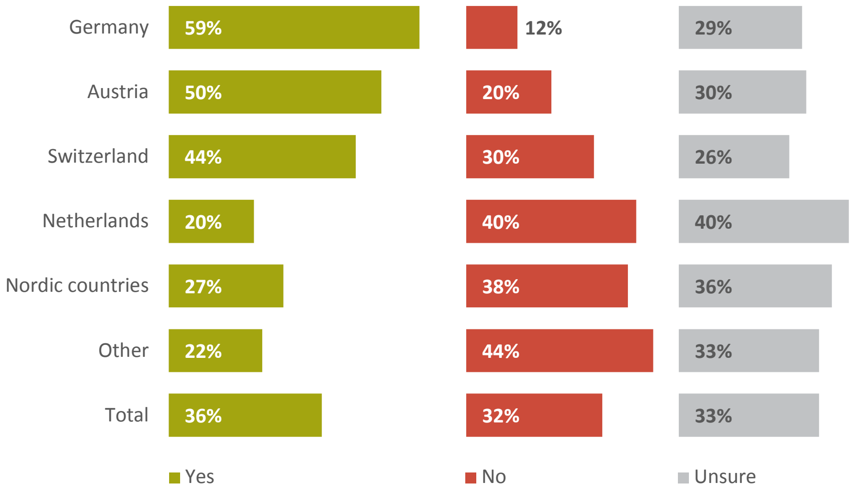
Those results are in line with findings from the “HIMSS Analytics Quick HIT Survey: Ransomware” in the United States (5% would pay the ransom).

> *“Most probably the decision will be determined by various factors, including the scale of the attack, when it was detected, how quickly the business continuity plan kicked in, how widespread the encryption is, and if so, when exactly the last data back-up occurred.”*
> (Brendan FitzGerald, HIMSS Analytics Research Director for Advisory Solutions: www.healthcareitnews.com; April 2016)

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; only employed in a health facility; Germany: n=39; Austria: n=44; Switzerland: n=67; Netherlands: n=28; Nordic countries: n= 41; Other: n=32; Total: n=251; Quick HIT Survey (US): www.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months refers to US hospitals

# RESULTS – PAYMENT OF RANSOM

**6. If hackers encrypted confidential data from a care provider organisation, do you think they would pay the ransom to get the data decoded?** [only participants who not are working in a health facility]



Respondents (all European countries combined) NOT working in a health facility are split into three nearly equally large groups:
One in three thinks that care providers would pay a ransom to cyber criminals. Another one in three thinks that they would not, and yet another one in three is unsure if care providers would pay.

This perception varies quite much by country. While in Germany a large majority (59%) thinks that care providers in their country would pay a ransom, only 20% of their neighbours from the Netherlands are of the same opinion.

If cyber criminals have the same perception it might not be surprising why German care providers have been the prime cyber attack target over the past months.

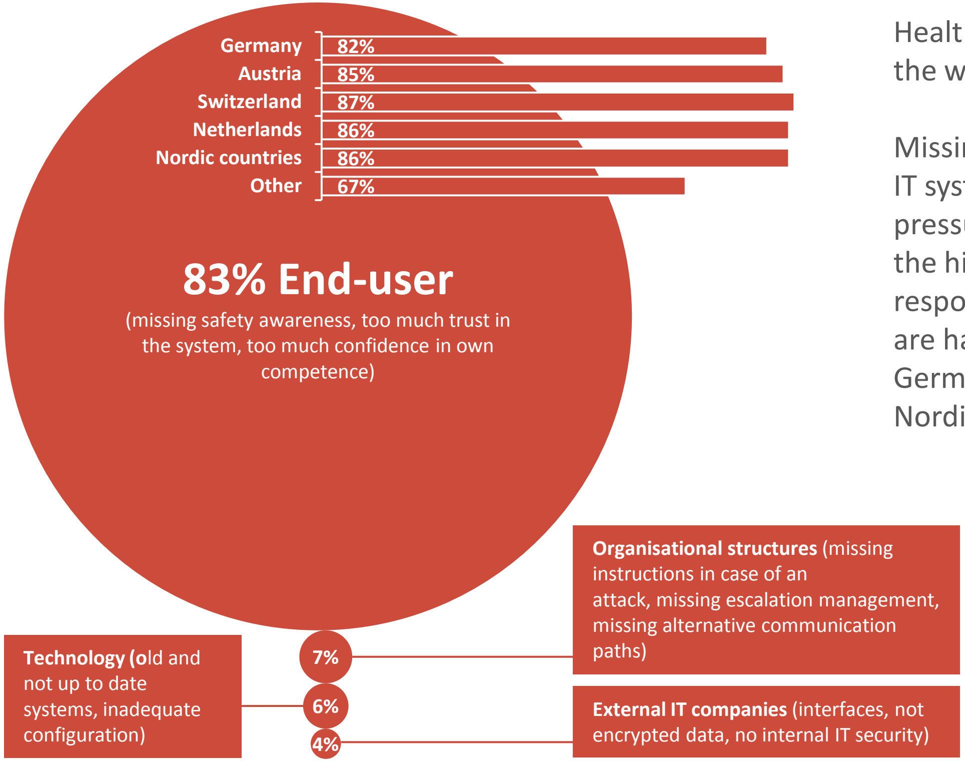
Please note that these results are based on a relatively small sample size when separated by country. While not being on very firm ground they can be seen as indicative.

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; only not employed in a health facility; Germany: n=17; Austria: n=10; Switzerland: n=27; Netherlands: n=15; Nordic countries: n=45; Other: n=9

# RESULTS – WEAKEST SPOT FOR ATTACKS

## 7. What do you think is the weakest spot for your organisation in terms of cyber-attacks?

[only participants who are working in a health facility]



**83% End-user**
(missing safety awareness, too much trust in the system, too much confidence in own competence)

**Organisational structures** (missing instructions in case of an attack, missing escalation management, missing alternative communication paths)

**Technology (**old and not up to date systems, inadequate configuration)

**External IT companies** (interfaces, not encrypted data, no internal IT security)

Health facility employees identify human errors as the weakest spot to data security.

Missing safety awareness and training, blind trust in IT systems, self-confidence in doing things right, time pressure and other factors turn the "end user" into the highest risk factor for data security. 83% of respondents are of that opinion. In this aspect there are hardly any noticeable differences between Germany, Austria, Switzerland, Netherlands and the Nordic countries.

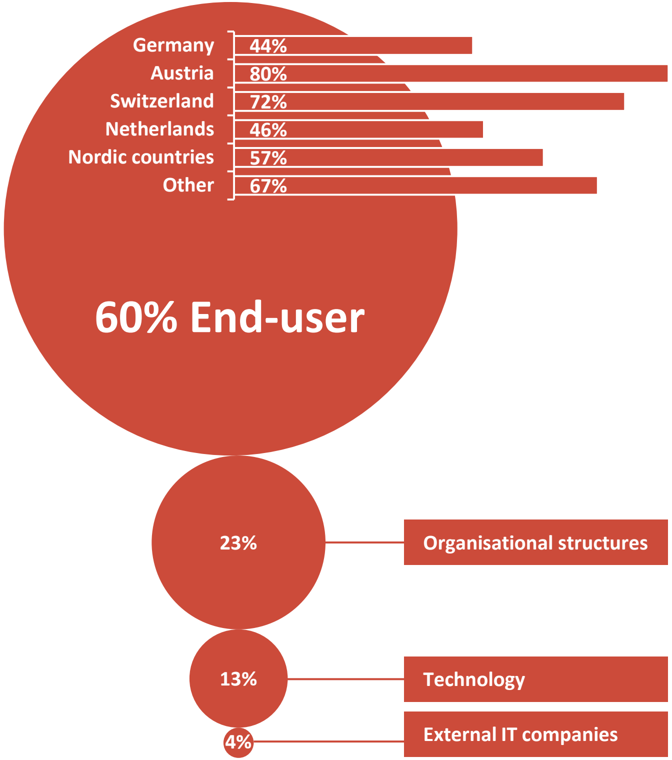
Other risk factors play a minor role. "Organisational structures" (Total: 7%), "Technology" (Total: 6%) or "External IT companies" (Total: 4%) are trailing far behind in risk perception.

Source: HIMSS Analytics; Study „eHealth trend barometer"; Survey period July to August 2016; only employed in a health facility; Total: n=220; most common response "End-user" Germany: n=28, Austria: n=29, Switzerland: n=53, Netherlands: n=24, Nordic countries: n=31, Other: n=18

# RESULTS – WEAKEST SPOT FOR ATTACKS

## 8. What do you think is the weakest spot for care provider organisations in terms of cyber-attacks?

[only participants who not are working in a health facility]



The perception about cyber-attack risk factors of non-health facility respondents differs to some extent from health facility employees. Only 60% of respondents (Total) not working in a health facility see the “end-user” as the weakest spot.

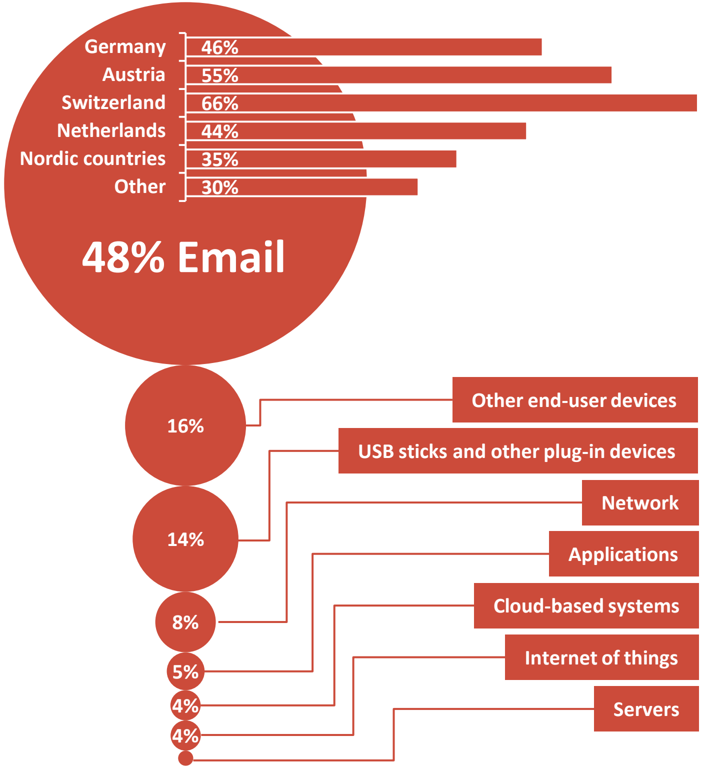
From an external perspective, i.e. from someone not working in a health facility, organisational structures are perceived to being relatively unsafe, 23% of respondents are of this opinion (vs. 7% from health facility employees). This includes things like missing instructions in case of an attack, missing escalation management and missing alternative communication paths.

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; only not employed in a health facility; Total: n=115; most common response “End-user” Germany: n=7, Austria: n=8, Switzerland: n=18, Netherlands: n=6, Nordic countries: n=24, Other: n=6

# RESULTS – AREA OF VULNERABILITY

### 9. In terms of IT environment in your organisation: What is the greatest area of vulnerability for attacks?

[only participants who are working in a health facility]



Having a closer look at the IT environment in a health facility almost every second respondent working in those organisations named email as the area with the greatest vulnerability for attacks (Total: 48%).

End-user devices (e.g. Laptops, Tablets, Smartphones) as well as thumb drives (such as USB sticks) are the next largest risks according to survey respondents.

These findings correspond quite well with the “human risk factor” identified earlier on. Email, end-user devices, USB sticks are key work tools for clinicians. A well defined IT security strategy needs to encompass People, Technology and Processes.

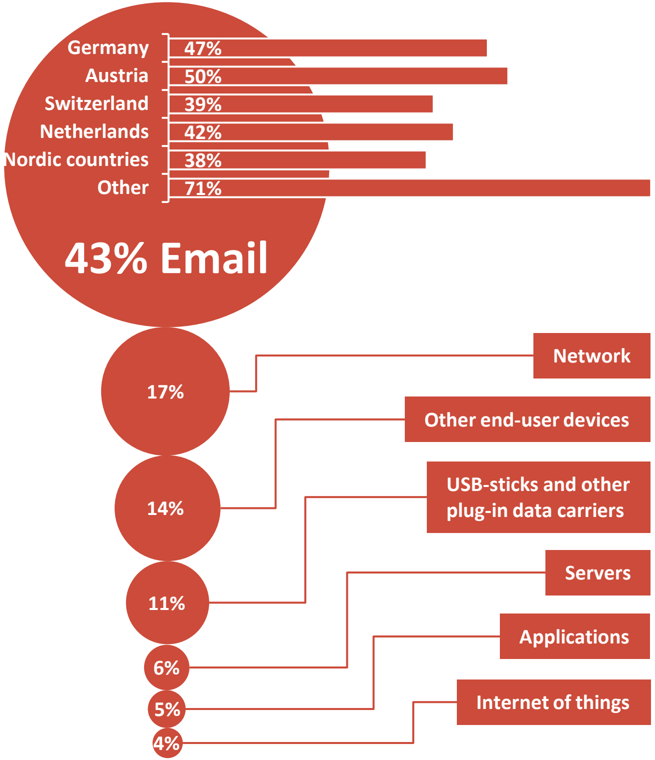
Contrary to concerns often raised about Cloud Computing, only few survey respondents (4%) perceive this as a significant risk. Perhaps also because this is still used relatively rarely in health organisations.

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; only employed in a health facility; Total: n=219; most common response “Email” Germany: n=17, Austria: n=18, Switzerland: n=38, Netherlands: n=12, Nordic countries: n=12, Other: n=9

# RESULTS – AREA OF VULNERABILITY

**10. In terms of IT environment in a care provider organisation: What is the greatest area of vulnerability for attacks?**

[only participants who not are working in a health facility]



Respondents who are not working in a health facility share the opinion with health facility employees that email communication is the largest area of vulnerability in the IT environment (Total „Email“: 43%).

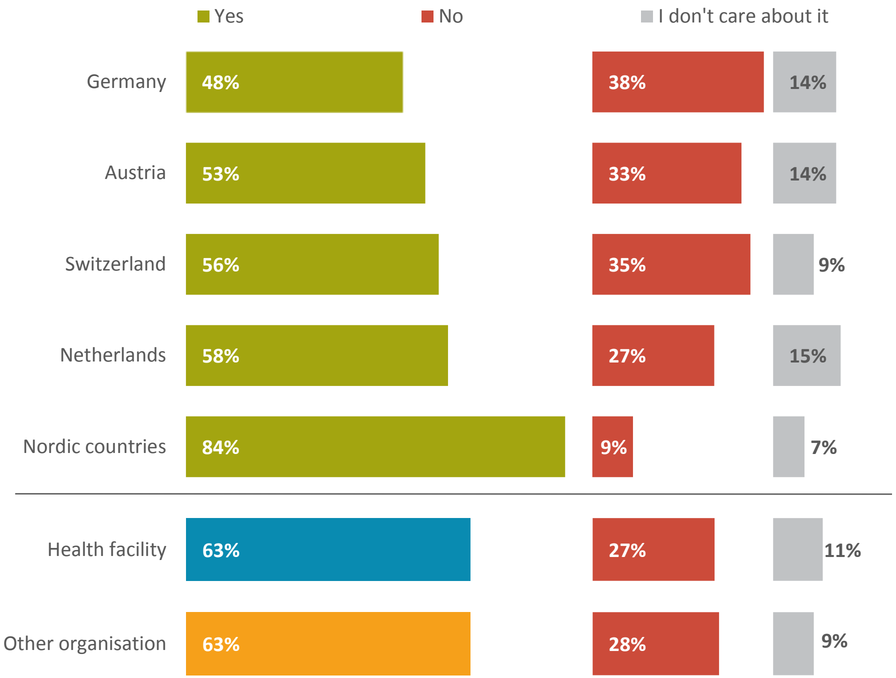
The largest difference between the two groups can be found in the category "Network", which twice as many non-health facility respondents perceive as the largest risk (17% vs. 8%). Corrupted links, misconfigured router and man-in-the-middle attacks are examples for this quite complex category.

Due to the relatively small sample size of this respondent group differences between response shares under 20% should be interpreted with caution.

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; only not employed in a health facility; Total: n=106; most common response "Email" Germany: n=7, Austria: n=5, Switzerland: n=9, Netherlands: n=5, Nordic countries: n=15, Other: n=5

# RESULTS – DATA PROTECTION

## 11. In your individual role as a patient: Is your personal health information adequately protected by health care providers in your country?



This survey confirms the often raised impression that Germans are the citizens mostly concerned about the protection of their data. Only 48% of German respondents feel that their health data is adequately protected (and 38% feel it is not). As a matter of fact the other two German-speaking countries (Austria and Switzerland) fall in that same group of “mostly concerned” countries.

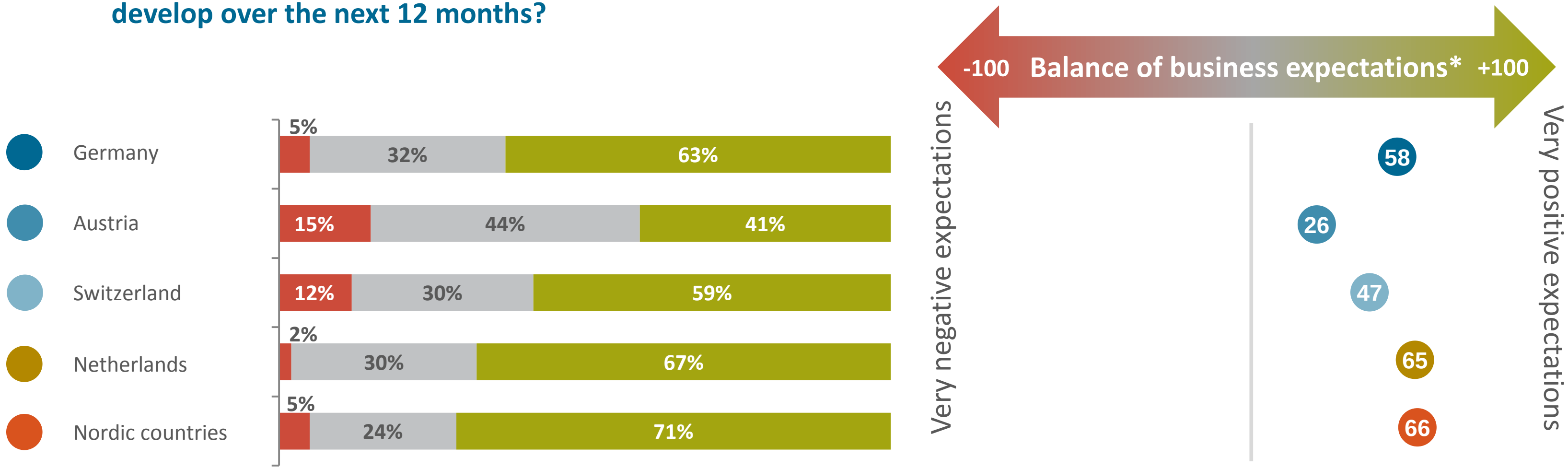
The situation is clearly different in the Nordic countries where only 9% of respondents feel that their health data is not well-enough protected.

This is particularly noteworthy since health services in the Nordic countries are typically quite more digitised (and thus potentially more prone to get “hacked”) than in the DACH region. Culture seems to have a significant influence – and perhaps larger impact than technology and security measures – on the level of comfort with data protection

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; Germany: n=42, Austria: n=43, Switzerland: n=68, Netherlands: n=33, Nordic countries: n=75; Valid cases for working in a health facility: n=195 including “Other” countries; Valid cases for working in a other organisation facility: n=93 including “Other” countries

# RESULTS – BUSINESS EXPECTATIONS

## 12. How will the environment for eHealth innovation and investment in your country develop over the next 12 months?



**Business prospects for the eHealth sector continue to be very positive.**

By far the best expectations were given by participants from the Nordic countries (Balance of business expectations: 66), which is a decrease of 8 points in comparison to the last survey wave of the “eHealth trend barometer” (survey period: Q1 2016; Balance of business expectations: 74). Slightly behind the expectations from the Dutch respondents (Balance of business expectations: 65). Austrian respondents do have more restrained expectations (Balance of business expectations: 26) like last time (survey period: Q1 2016; Balance of business expectations: 26).

Source: HIMSS Analytics; Study „eHealth trend barometer“; Survey period July to August 2016; without “Don’t know”; without “Other” countries; Germany: n=56; Austria: n=54; Switzerland: n=94; Netherlands: n=43; Nordic countries: n=86; *Score: “Balance of business expectations” = (percentage “improve” – percentage “worse”)*100

# Thank you for your participation!

HIMSS Analytics
Office Leipzig
Schwägrichenstraße 9
04107 Leipzig
Germany

www.himss.eu/analytics
www.himssanalytics.org

Join the European eHealth community panel
**info@himssanalytics.eu**

eHEALTH
TRENDBAROMETER