Security Awareness Workshop

SWITCH

Katja, Nathalie, Antoine, Michael
katja.doerlemann@switch.ch

Zürich, August 16th 2018

Agenda

09h30-10h00	Welcome coffee
10h00-10h30	**General introduction** Katja Dörlemann, SWITCH
10h30-11h00	**Security and the Internet: an ongoing struggle?** Michael Hausding, SWITCH
11h00-11h30	**Cyber risk scenarios at universities** Antoine Neuenschwander, SWITCH
11h30-12h00	**Security Awareness and e-learning** Katja Dörlemann, SWITCH
12h00-13h00	**Sandwich lunch** Offered by SWITCH
13h00-14h00	**Security painpoints discussion**
14h00-14h15	Coffee break
14h15-15h15	**Security painpoints presentation**
15h15-15h30	Summary & outlook Katja Dörlemann, SWITCH

What’s new @ SWITCH Q3/18

- **Digital Solutions & Consulting Services**

  Development of a new business division and creation of a sustainable business case for the Community Service Hub
  marco.duetsch@switch.ch, https://swit.ch/dscs

- **FUTURE UNIVERSITY**

  Think Tank SWITCH in partnership with W.I.R.E.
  Read our story, download poster, order study
  swit.ch/future-university/order
  swit.ch/future-university/story

- **Coordination office on scientific information**

  Conceptional work together with swissuniversities
  andreas.dudler@switch.ch

- **Procurement**

  Adobe Framework Agreement and Microsoft Data Processing Amendment (DPA) signed
  procurement@switch.ch

  4th Higher Education Cloud Day, 28 August 2018
  Registration www.switch.ch/procure/4thhecd/

- **SLSP @ SWITCH**

  Subtenants from 1 March 2018 at SWITCH premises
  christine.lanner@switch.ch

What’s new @ SWITCH Q3/18

Security

- **SWITCH Security Awareness Day**
  - 24 October 2018, Haus der Universität Berne
    https://swit.ch/securityawarenessday
    Password: SWITCHAwareness2018

- **SWITCH-CERT**
  - Mattermost, a secure chat for NREN
    cert@switch.ch

- **Malware / Phishing**
  - New contact
    spamreport@post.switch.ch
    spamanalysis@post.switch.ch

- **SWITCH Security Blog**
  - Read our Blog
    https://securityblog.switch.ch

Network

- **SWITCHlan Service Description**
  - From July 1st a new service description is available
    https://portal.switch.ch/vip/services/lan/
    daniel.bertolo@switch.ch

- **Big Data Transfer Community**
  - Interdisciplinary network and security workshop together with higher education
    daniel.bertolo@switch.ch, silvio.oertli@switch.ch
    martin.leuthold@switch.ch

- **IoT Working Group**
  - Interdisciplinary (researchers, network, security) community together with higher education
    kurt.baumann@switch.ch, daniel.bertolo@switch.ch

- **SWITCH IoT ecosystem**
  - SWITCH creates a base for a strong IoT ecosystem in partnership with ONIA
    www.switch.ch/stories/iot-day-2018/

What’s new @ SWITCH Q3/18

Trust & Identity

- **SWITCH edu-ID**
  - Deployment step 3 + 4 in August
    christoph.graf@switch.ch
  - Non-profit member of “The OpenID Foundation”
    openid.net/foundation/sponsoring-members

- **Identity Blog**
  - Read our Blog
    identityblog.switch.ch

Infrastructure & Data Services

- **SWITCHengines**
  - are now qualified for SNF and Innosuisse funding
  - storage and data solutions started with universities
  - Admin UI enhancement: self-signup & virtual classroom
  - P-5 long term storage project submitted

  konrad.jaggi@switch.ch, switch.ch/engines

- **IT for Research Day 2018**
  - 19 September 2018, University of Berne

  swit.ch/researchday2018

Let’s shed some light on Security

CERT

Computer Emergency Response Team

What does a CERT do?

SWITCH-CERT offers a variety of high quality security services to help protecting our customers critical ICT infrastructure. Our services ensure customers readiness and allow rapidly react during a security crisis. We aim at preventing issues and reduce damage during attacks.

SWITCH’s Computer Emergency Response Team is the first point of contact for customers with IT security issues. Most of the time, it learns of problems before its customers do and starts working to fix them immediately. Thanks to its worldwide network of partners, SWITCH-CERT effectively handles incidents across national borders.

What does a CERT do?

SWITCH-CERT offers a variety of high quality security services to **help protecting our customers critical ICT infrastructure**. Our services ensure customers readiness and allow rapidly react during a security crisis. We aim at **preventing issues and reduce damage during attacks**.

SWITCH’s Computer Emergency Response Team is the first point of contact for customers with IT security issues. Most of the time, it learns of problems before its customers do and starts working to fix them immediately. Thanks to its worldwide network of partners, SWITCH-CERT effectively **handles incidents across national borders**.

SWITCH-CERT

22 years SWITCH-CERT – infor and trusted community

Customers

- Universities
- Hospitals
- Banks

Services

Cyber Threat Intelligence, Detection, Incident and Response as core competences

- Computer Security Incident Response
- Network Security Monitoring
- Trusted Collaboration Services
- Malware Monitoring & Analysis
- Malicious Domain Takedown
- Information & Awareness Services
- DNS Firewall Service

Your benefits

Comprehensive incident support and optimal network security, especially for the Swiss Internet

SWITCH-CERT: Who is it?

Silvio

Frank

Antoine

Slavo

Michael

Mathias

Andreas

Daniel

Yves

Matthias

Oli

Michael

Jakob

Katja

SWITCH-CERT: Who is it?

Network Security Engineer

Antoine

Silvio

Frank

Slavo

Michael

Competence Lead DNS & Domain Abuse

Mathias

Yves

Andreas

Daniel

Matthias

Oli

Jakob

Katja

Security Awareness Specialist

Michael

Security?

Google image search: security

Many different types of security

- Internet Security
- Cyber Security
- Information Security
- Data security

Google image search: internet security

Google image search: cyber security

Google image search: information security

Google image search: data security

Security is all about padlocks.

Security is all about padlocks?

Let’s talk about

Sicherheit

Sécurité

Sicurezza

Security Awareness and e-learning

SWITCH

Katja Dörlemann
katja.doerlemann@switch.ch

Zürich, August 16th 2018

Don’t be scared –

Your IT (security) team protects you

Don’t be scared –

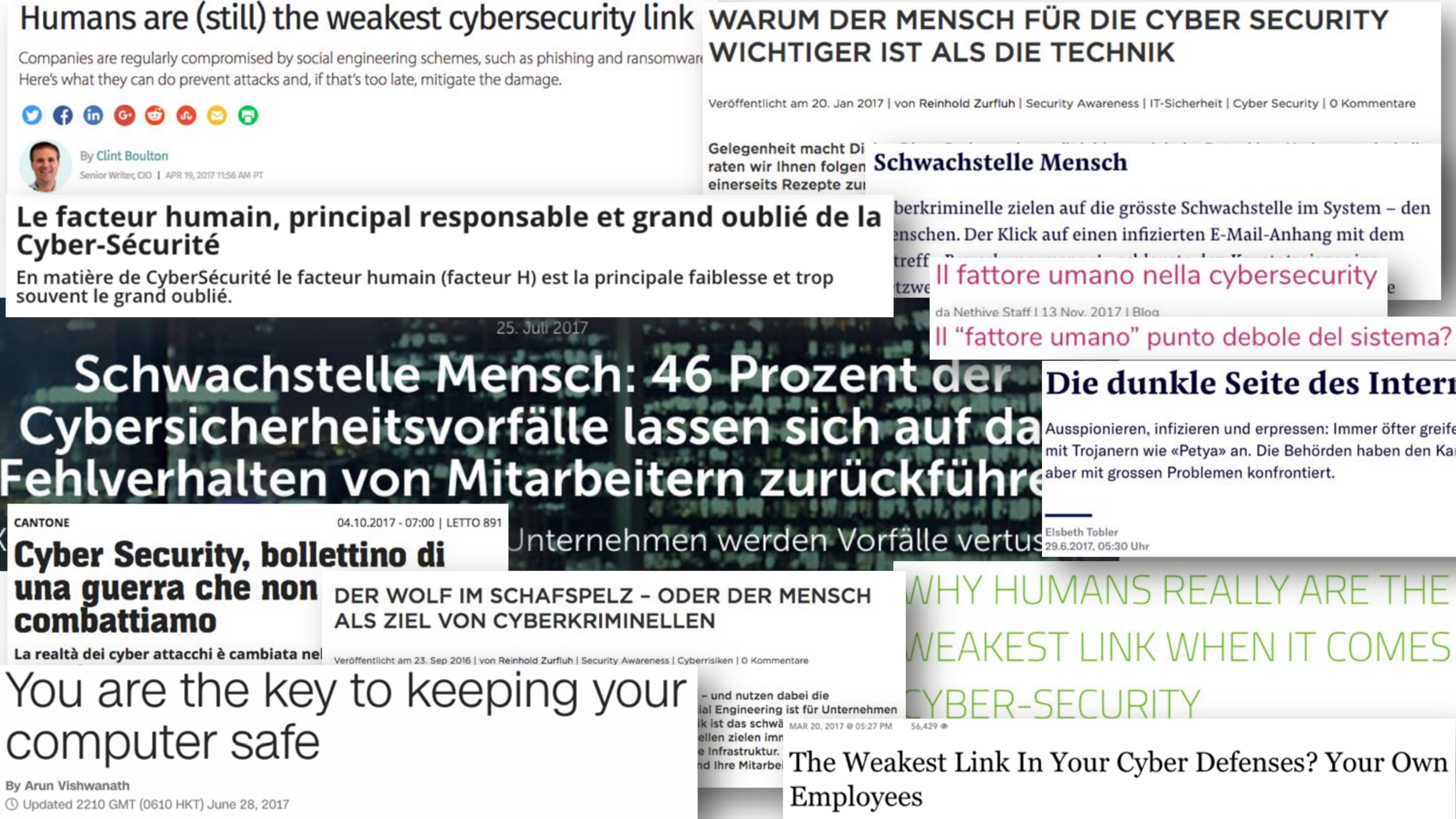
Your IT (security) team protects you

…from most of it

What are Security Threats?

Google image search: security threats

What are Security Threats?



Humans are (still) the weakest cybersecurity link

Companies are regularly compromised by social engineering schemes, such as phishing and ransomware
Here's what they can do prevent attacks and, if that's too late, mitigate the damage.

By Clint Boulton
Senior Writer, CIO | APR 19, 2017 11:56 AM PT

WARUM DER MENSCH FÜR DIE CYBER SECURITY WICHTIGER IST ALS DIE TECHNIK

Veröffentlicht am 20. Jan 2017 | von Reinhold Zurfluh | Security Awareness | IT-Sicherheit | Cyber Security | 0 Kommentare

Gelegenheit macht Di
raten wir Ihnen folgen
einerseits Rezepte zu

Schwachstelle Mensch

berkriminelle zielen auf die grösste Schwachstelle im System – den
nschen. Der Klick auf einen infizierten E-Mail-Anhang mit dem
treff
tzwe

Le facteur humain, principal responsable et grand oublié de la Cyber-Sécurité

En matière de CyberSécurité le facteur humain (facteur H) est la principale faiblesse et trop souvent le grand oublié.

Il fattore umano nella cybersecurity

da Nethive Staff | 13 Nov, 2017 | Blog

Il "fattore umano" punto debole del sistema?

25. Juli 2017

Schwachstelle Mensch: 46 Prozent der Cybersicherheitsvorfälle lassen sich auf da
Fehlverhalten von Mitarbeitern zurückführe

Unternehmen werden Vorfälle vertus

Die dunkle Seite des Intern

Ausspionieren, infizieren und erpressen: Immer öfter greife
mit Trojanern wie «Petya» an. Die Behörden haben den Ka
aber mit grossen Problemen konfrontiert.

Elsbeth Tobler
29.6.2017, 05:30 Uhr

CANTONE 04.10.2017 - 07:00 | LETTO 891

Cyber Security, bollettino di una guerra che non combattiamo

La realtà dei cyber attacchi è cambiata nel

DER WOLF IM SCHAFSPELZ – ODER DER MENSCH ALS ZIEL VON CYBERKRIMINELLEN

Veröffentlicht am 23. Sep 2016 | von Reinhold Zurfluh | Security Awareness | Cyberrisiken | 0 Kommentare

- und nutzen dabei die
ial Engineering ist für Unternehmen
ik ist das schwä
ellen zielen imm
e Infrastruktur.
nd Ihre Mitarbei

WHY HUMANS REALLY ARE THE WEAKEST LINK WHEN IT COMES CYBER-SECURITY

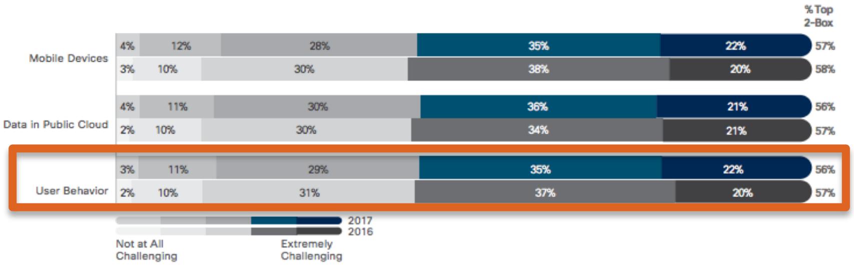
You are the key to keeping your computer safe

By Arun Vishwanath
Updated 2210 GMT (0610 HKT) June 28, 2017

MAR 20, 2017 @ 05:27 PM 56,429

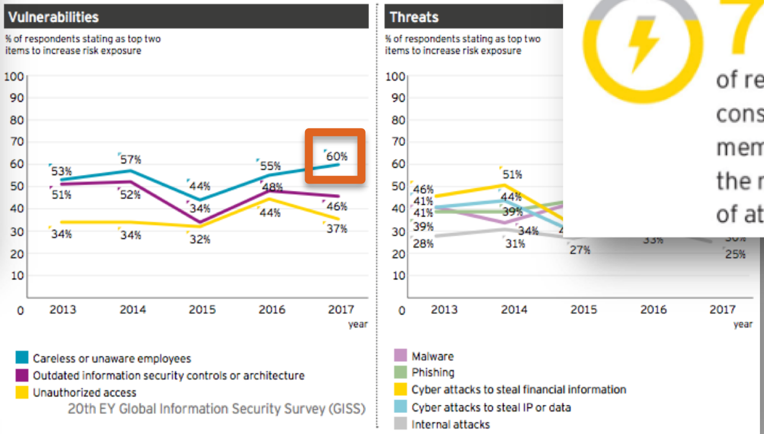
The Weakest Link In Your Cyber Defenses? Your Own Employees

Figure 41 Most challenging areas to defend: mobile devices and cloud data



Cisco 2018
Annual Cybersecurity Report

Threats and vulnerabilities perceived to have most the risk exposure of the respondents, 2013-2017

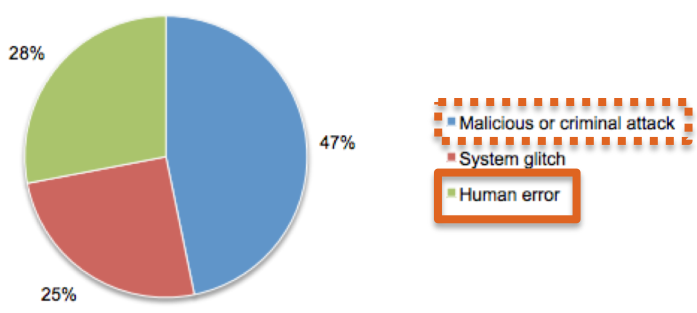


20th EY Global Information Security Survey (GISS)

77%

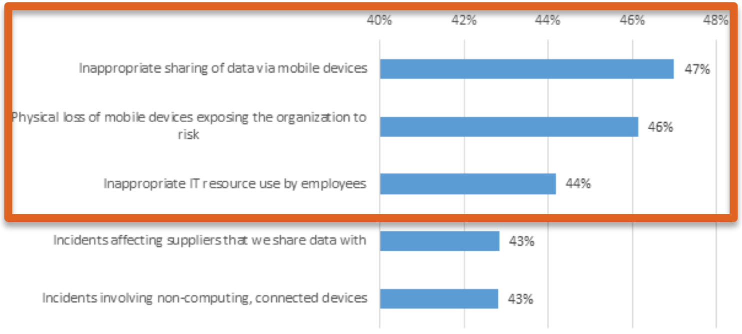
of respondents consider a careless member of staff as the most likely source of attack.

Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach



Ponemon Institute
2017 Cost of Data Breach Study

Where do businesses feel vulnerable? Top five fears



Source: IT Security Risks Survey 2017, global data

SECURITY AWARENESS shall fix it all

What is Security Awareness?

Google image search: security awareness

In theory, Security Awareness is…

ISO 27000:2016:
…"[one of the] fundamental principles [that] contribute to the successful implementation of an ISMS".

wikipedia:
…"the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization."

NIST SP800-50:
…"not training. The purpose of awareness presentations is simply to focus attention on security."

OECD Guidelines for the Security of Information Systems and Networks:
…"the first line of defence for the security of information systems and networks."

Security Awareness is…

ISO 27000:2016:
…“[one of the] fundamental principles [that] contribute to the successful implementation of an ISMS”.

wikipedia:
…“the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.”

NIST SP800-50:
…”not training. The purpose of awareness presentations is simply to focus attention on security.

OECD Guidelines for the Security of Information Systems and Networks:
…“the first line of defence for the security of information systems and networks.”

Note:

1. Security Awareness is very important!
2. Security Awareness measures shall make users aware of security issues.
3. Security Awareness measures shall transmit sustainable knowledge about information security.

Resources for Security Awareness

SANS SECURITY AWARENESS

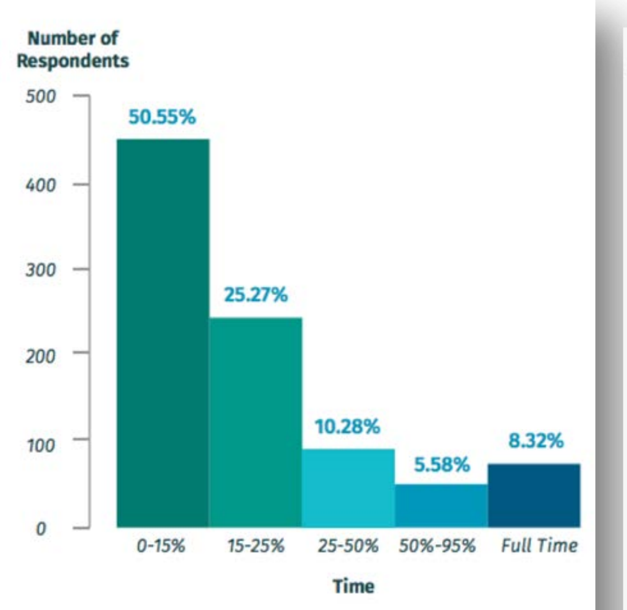
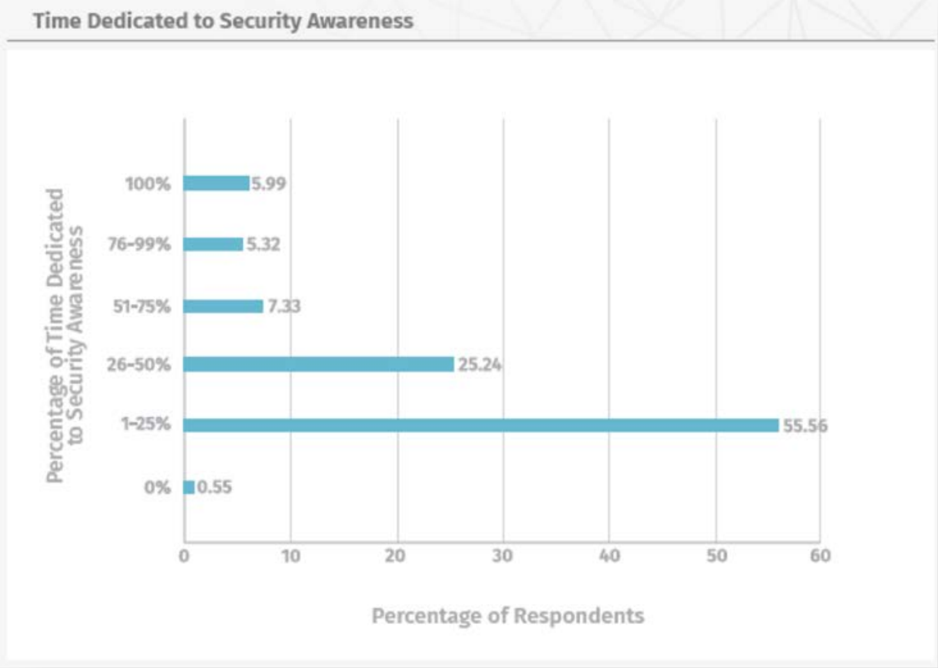


Fig. 7 - What percentage of your time is focused on security awareness?

Time Dedicated to Security Awareness



Security Awareness Trinity

Awareness

Raising interest and focusing attention on a topic

Education

Learning new skills and the theory behind it

Training

Learning and training (new) skills

Responsible for Security Awareness

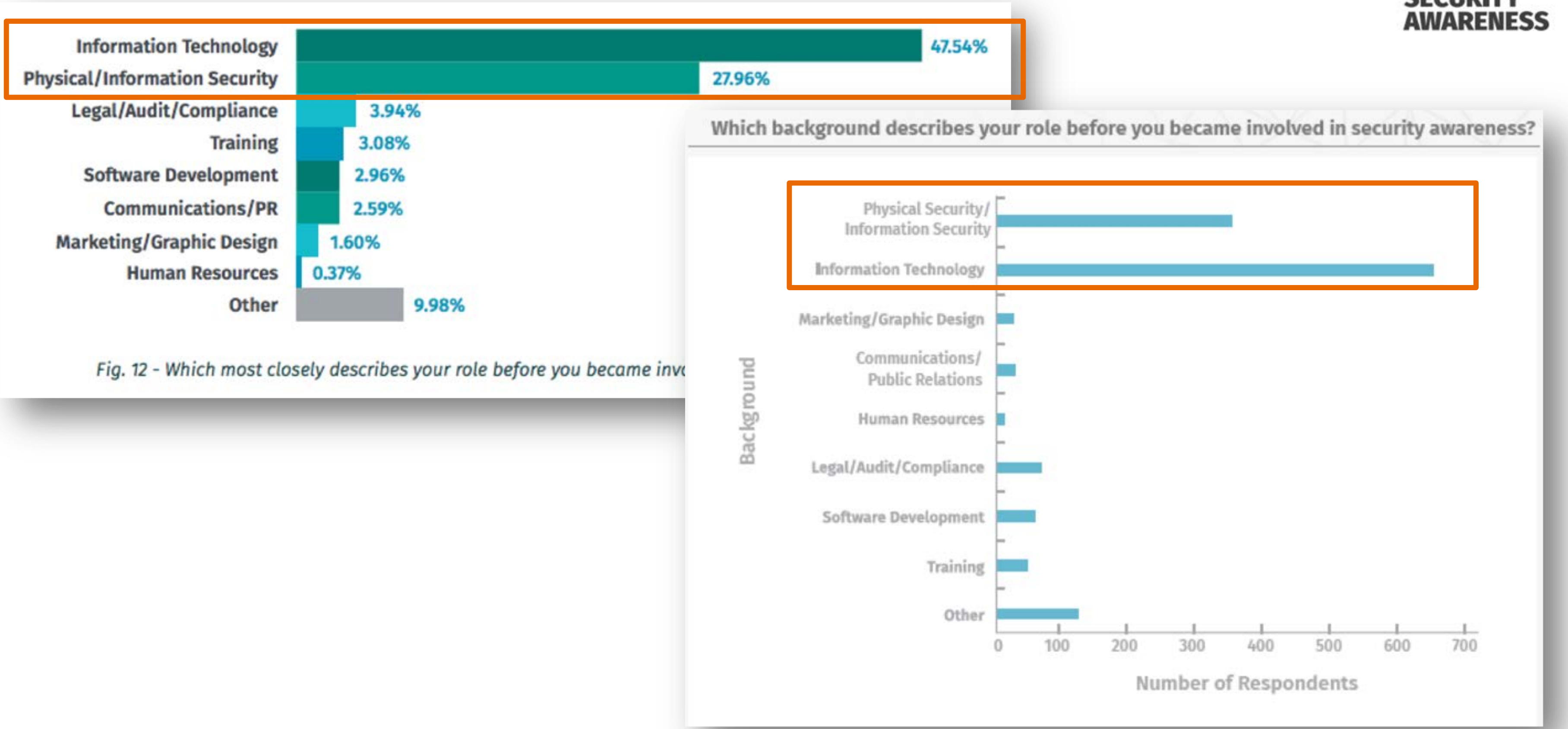
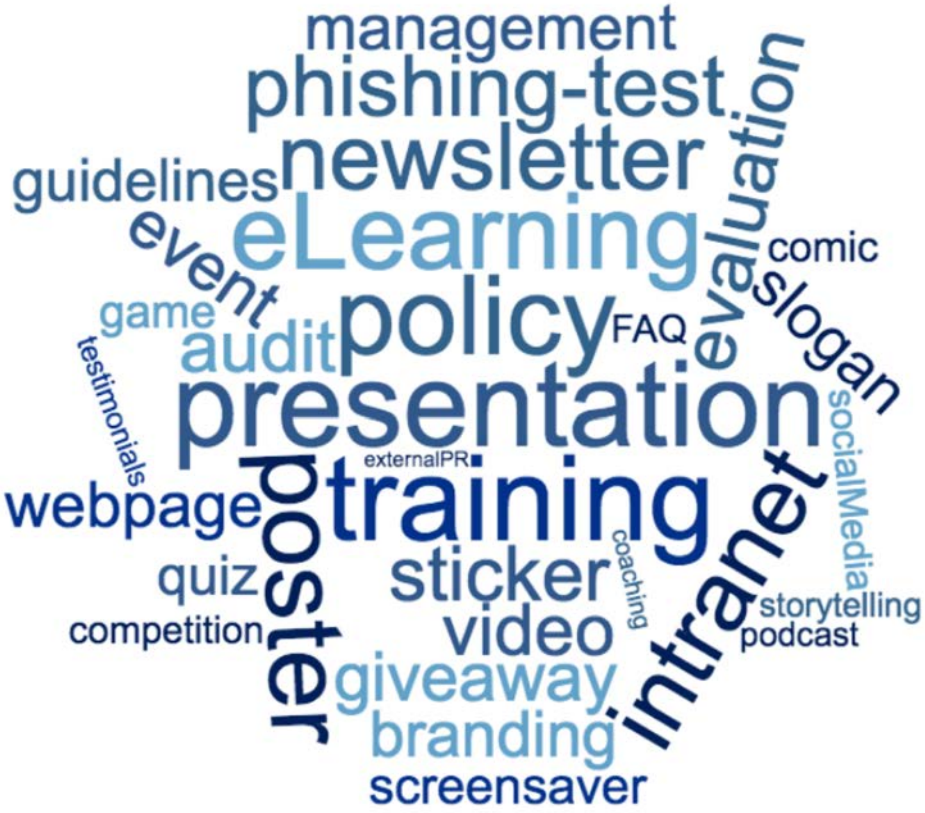


Fig. 12 - Which most closely describes your role before you became inv

Which background describes your role before you became involved in security awareness?

> *The geeks have inherited awareness (is that good?).*
>
> – SANS Security Awareness Report

Security Awareness in real life



The biggest challenges

1. **Missing communication skills**
2. **Missing employee and management support**
3. **Few financial and personal resources**

e-learning and
the fight against cyber crime

Joining forces!

Security Awareness Trinity

Awareness

Raising interest and focusing attention on a topic

Education

Learning new skills and the theory behind it

Training

Learning and training (new) skills

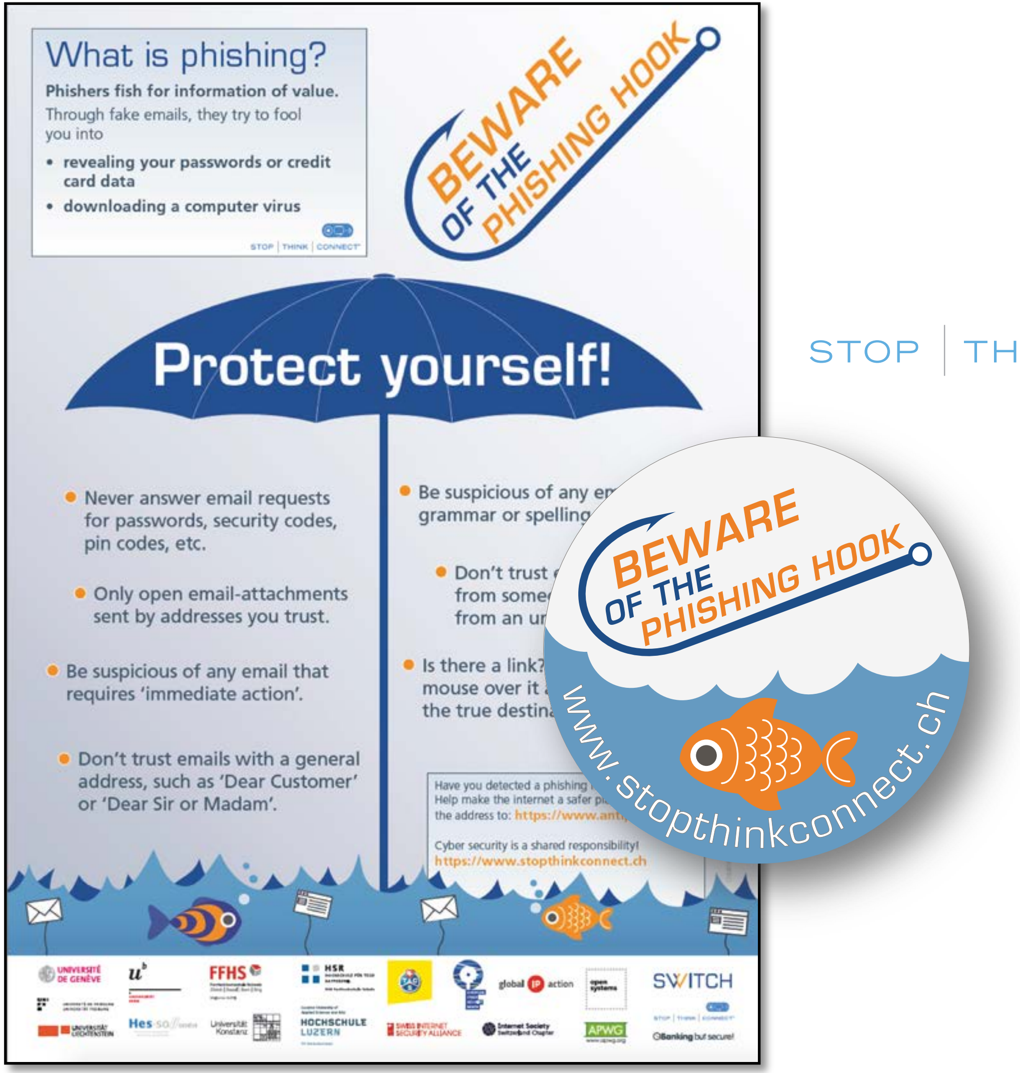
1. **Missing communication skills**
2. **Missing employee and management support**
3. **Few financial and personal resources**

1. Support your local IT (Security) Team

2. Include «Cyber Security» in your education strategy

Collaboration/Working Groups with security teams

SWITCH



What is phishing?

Phishers fish for information of value.

Through fake emails, they try to fool you into

- **revealing your passwords or credit card data**
- **downloading a computer virus**

STOP | THINK | CONNECT

BEWARE OF THE PHISHING HOOK

Protect yourself!

- Never answer email requests for passwords, security codes, pin codes, etc.
- Only open email-attachments sent by addresses you trust.
- Be suspicious of any email that requires 'immediate action'.
- Don't trust emails with a general address, such as 'Dear Customer' or 'Dear Sir or Madam'.
- Be suspicious of any em grammar or spelling
- Don't trust e from some from an ur
- Is there a link? mouse over it the true destin

Have you detected a phishing
Help make the internet a safer pl
the address to: https://www.anti

Cyber security is a shared responsibility!
https://www.stopthinkconnect.ch

STOP | THINK | CONNECT™

Non ricordi le password?
Cantale!
Per maggiori informazioni
www.stopthinkconnect.ch

ty Alliance (SISA)

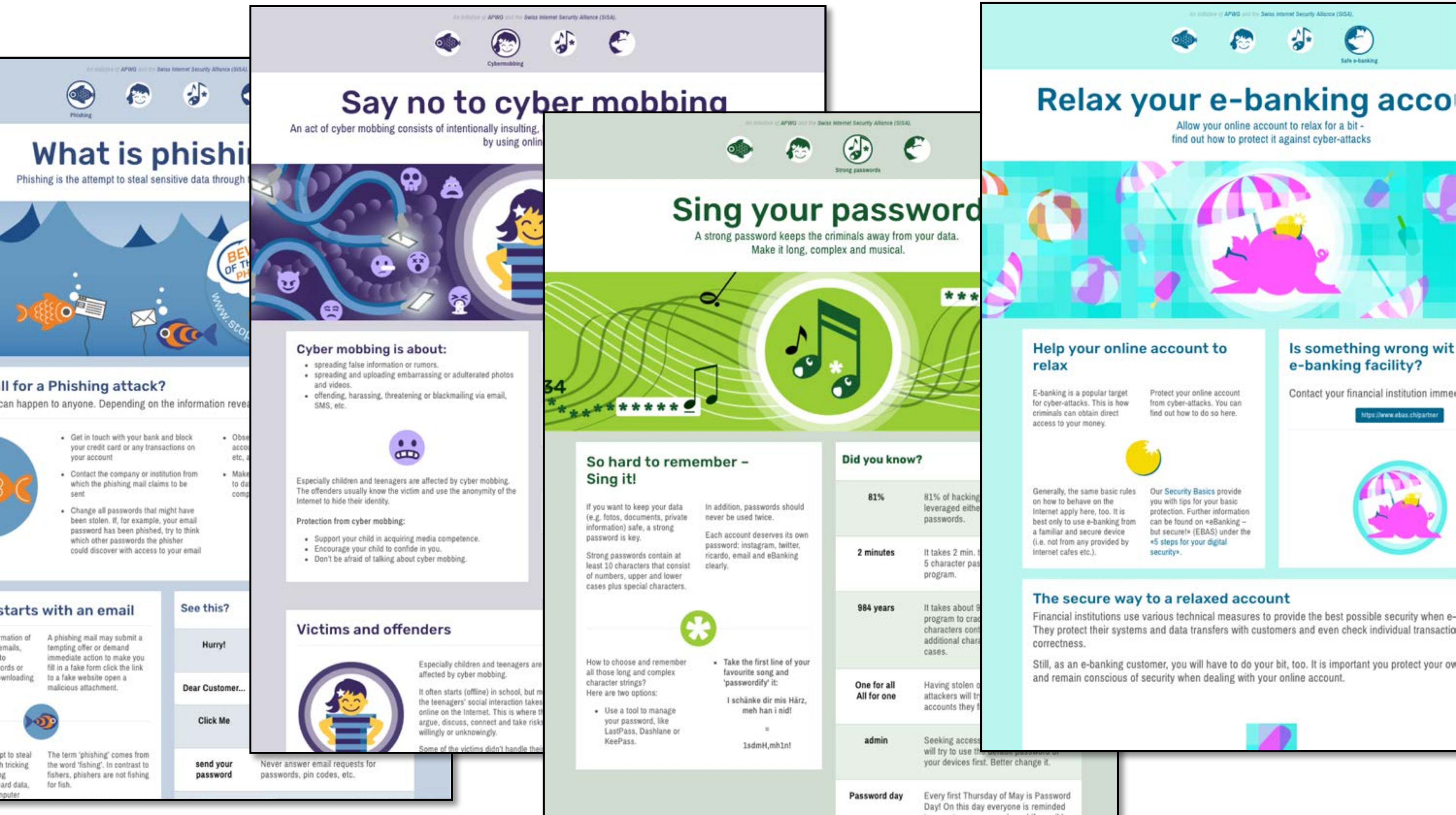
Sing your password

Chante ton mot de passe

Chanta tes pled-clav

Sing Dis Passwort

Canta la tua password



An initiative of APWG and the Swiss Internet Security Alliance (SISA).

What is phishi

Phishing is the attempt to steal sensitive data through t

ll for a Phishing attack?

can happen to anyone. Depending on the information revea

- Get in touch with your bank and block your credit card or any transactions on your account
- Contact the company or institution from which the phishing mail claims to be sent
- Change all passwords that might have been stolen. If, for example, your email password has been phished, try to think which other passwords the phisher could discover with access to your email

- Obse accou etc., a
- Make to da comp

starts with an email

mation of emails, to ords or wnloading

A phishing mail may submit a tempting offer or demand immediate action to ensure you fill in a fake form click the link to a fake website open a malicious attachment.

pt to steal h tricking g ard data, nputer

The term 'phishing' comes from the word 'fishing'. In contrast to fishers, phishers are not fishing for fish.

See this?

Hurry!	
Dear Customer...	
Click Me	
send your password	Never answer email requests for passwords, pin codes, etc.

An initiative of APWG and the Swiss Internet Security Alliance (SISA).

Say no to cyber mobbing

An act of cyber mobbing consists of intentionally insulting, by using onlin

Cyber mobbing is about:

- spreading false information or rumors.
- spreading and uploading embarrassing or adulterated photos and videos.
- offending, harassing, threatening or blackmailing via email, SMS, etc.

Especially children and teenagers are affected by cyber mobbing. The offenders usually know the victim and use the anonymity of the Internet to hide their identity.

Protection from cyber mobbing:

- Support your child in acquiring media competence.
- Encourage your child to confide in you.
- Don't be afraid of talking about cyber mobbing.

Victims and offenders

Especially children and teenagers are affected by cyber mobbing.

It often starts (offline) in school, but m the teenagers' social interaction takes online on the Internet. This is where th argue, discuss, connect and take risk willingly or unknowingly.

Some of the victims didn't handle thei

An initiative of APWG and the Swiss Internet Security Alliance (SISA).

Sing your password

A strong password keeps the criminals away from your data.
Make it long, complex and musical.

So hard to remember – Sing it!

If you want to keep your data (e.g. fotos, documents, private information) safe, a strong password is key.

Strong passwords contain at least 10 characters that consist of numbers, upper and lower cases plus special characters.

In addition, passwords should never be used twice.

Each account deserves its own password: instagram, twitter, ricardo, email and eBanking clearly.

How to choose and remember all those long and complex character strings?
Here are two options:

- Use a tool to manage your password, like LastPass, Dashlane or KeePass.
- Take the first line of your favourite song and 'passwordify' it:

I schänke dir mis Härz, meh han i nid!

=

1sdmH,mh1n!

Did you know?

81%	81% of hacking leveraged eithe passwords.
2 minutes	It takes 2 min. t 5 character pas program.
984 years	It takes about 9 program to crac characters cont additional chara cases.
One for all All for one	Having stolen c attackers will tr accounts they f
admin	Seeking access will try to use th default password of your devices first. Better change it.
Password day	Every first Thursday of May is Password Day! On this day everyone is reminded

An initiative of APWG and the Swiss Internet Security Alliance (SISA).

Relax your e-banking acco

Allow your online account to relax for a bit -
find out how to protect it against cyber-attacks

Help your online account to relax

E-banking is a popular target for cyber-attacks. This is how criminals can obtain direct access to your money.

Protect your online account from cyber-attacks. You can find out how to do so here.

Generally, the same basic rules on how to behave on the Internet apply here, too. It is best only to use e-banking from a familiar and secure device (i.e. not from any provided by Internet cafes etc.).

Our Security Basics provide you with tips for your basic protection. Further information can be found on «eBanking – but secure!» (EBAS) under the «5 steps for your digital security».

Is something wrong wit e-banking facility?

Contact your financial institution imme

https://www.ebas.ch/partner

The secure way to a relaxed account

Financial institutions use various technical measures to provide the best possible security when e- They protect their systems and data transfers with customers and even check individual transactio correctness.

Still, as an e-banking customer, you will have to do your bit, too. It is important you protect your ow and remain conscious of security when dealing with your online account.

>_Hack The Hacker

Unforgettable training

Hands-on security

https://swit.ch/hack-the-hacker

SWITCH Security Awareness Day

October 24th
Haus der Universität, Bern

09:30	**Welcome Coffee**	
10:00	**Introduction and agenda**	| Katja Dörlemann, SWITCH
10:15	**Security Awareness - New ways of thinking. An overview**	| Marcus Beyer, DXC Technologies
11:00	**Three critical concepts for measuring and improving security culture**	| Dr. Thomas Schlienger, TreeSolution
11:30	**The Websters - stories from the Internet**	| Alexandre Milan, BAKOM
12:00	**Lunch**	
13:30	**Awareness you can touch - theory and praxis**	| Dietmar Pokoyski, known_sense
15:00	**Coffee Break**	
15:30	**Security Awareness at University of Bern**	| Stefan Zahnd, University of Bern
16:00	**Security Awareness and civil society**	| Àngel Lopez, Cibervoluntarios
16:30	**Conclusion**	| Katja Dörlemann, SWITCH
16:45	**Apéro**	

Security Painpoints Discussion

SWITCH

Katja Dörlemann
katja.doerlemann@switch.ch

Zürich, August 16th 2018

Did you experience a security incident?

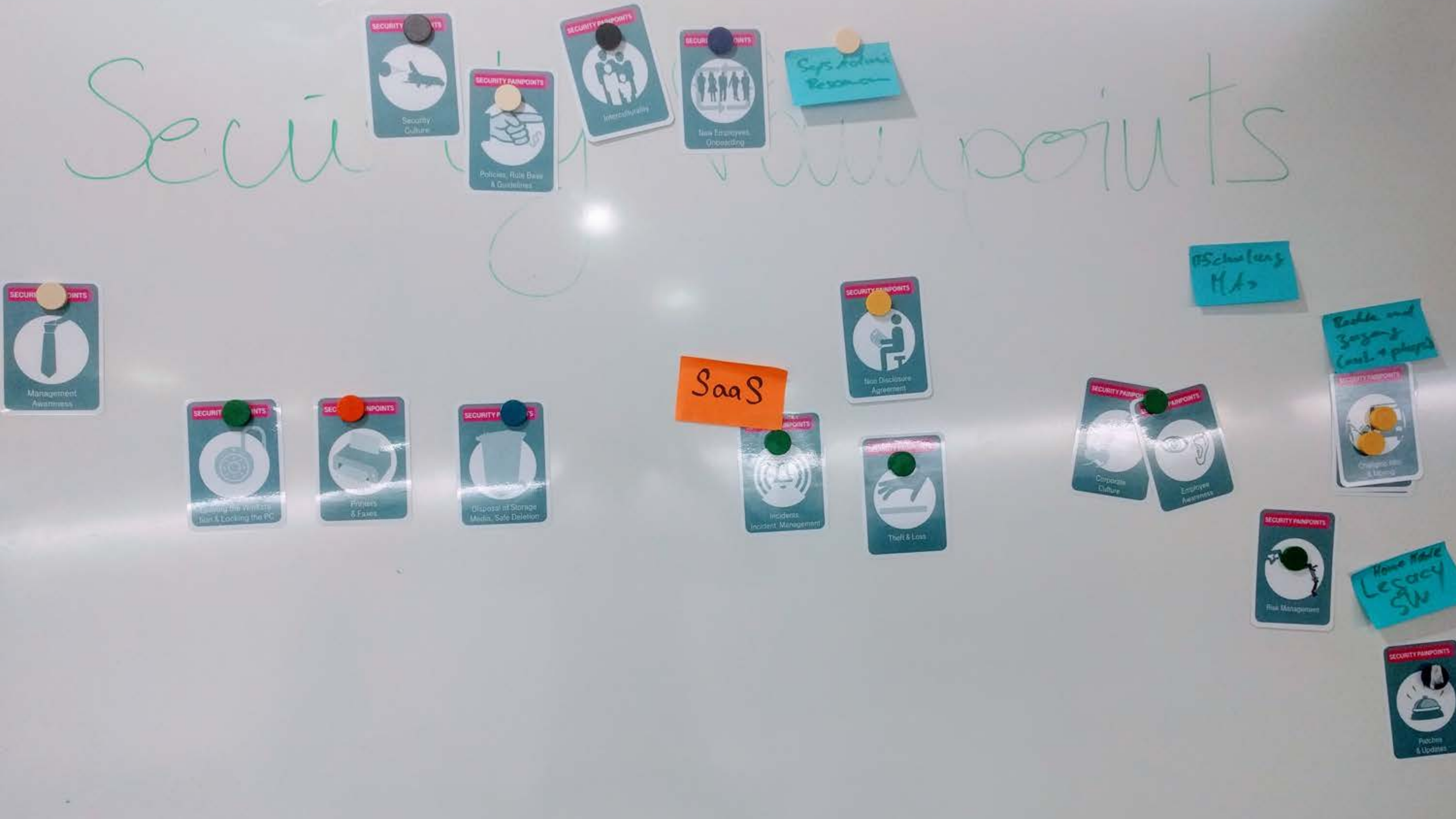
What are the Security Painpoints in your organisation?

Working questions

- What is important data?
- Who handles important data?
- Where do we store important data?
- If someone wanted to steal information, how could it happen?
- Who has access to our data?

Presentation:

Security Painpoints in your organisation


Security Painpoints
SECURITY PAINPOINTS
Security Culture
Policies, Rule Base & Guidelines
Interculturality
New Employees, Onboarding
Sys Admin Resource
Management Awareness
Leaving the Workstation & Locking the PC
Printers & Faxes
Disposal of Storage Media, Safe Deletion
SaaS
Incidents, Incident Management
Non Disclosure Agreement
Theft & Loss
ITSchulung MAs
Corporate Culture
Employee Awareness
Risk Management
Home Made Legacy SW
Patches & Updates

Summary and Outlook

SWITCH

Katja Dörlemann
katja.doerlemann@switch.ch

Zürich, August 16th 2018

Security?

- Security and the Internet: an ongoing struggle.
- Cyber risk scenarios at universities.
- Security Awareness and e-learning.
- Security and its painpoints.

Security!

Discussion and Questions

1. Support your local IT (Security) Team

2. Include «Cyber Security» in your education strategy

www.mentimeter.com