

A new awareness approach

Richard Verbrugge

30 September 2020

We cannot secure behaviour,
so employees need to behave securely.

How do we help them?

Previously

Awareness at ABN AMRO used to be “One Size Fits All”

Campaigns were identical for everyone using:

- Intranet, Connections
- E-mail
- Presentations
- Leaflets & posters
- Case stories
- Phishing tests
- E-learning



but, people are different

~~Awareness campaigns for everyone~~

To progress to a more
people centric awareness approach
we need information
on an individual level.



Problem:

What do employees know about Information Security and how do they behave now?

Education

How did we measure knowledge?

We used e-learnings to teach employees about Information Security

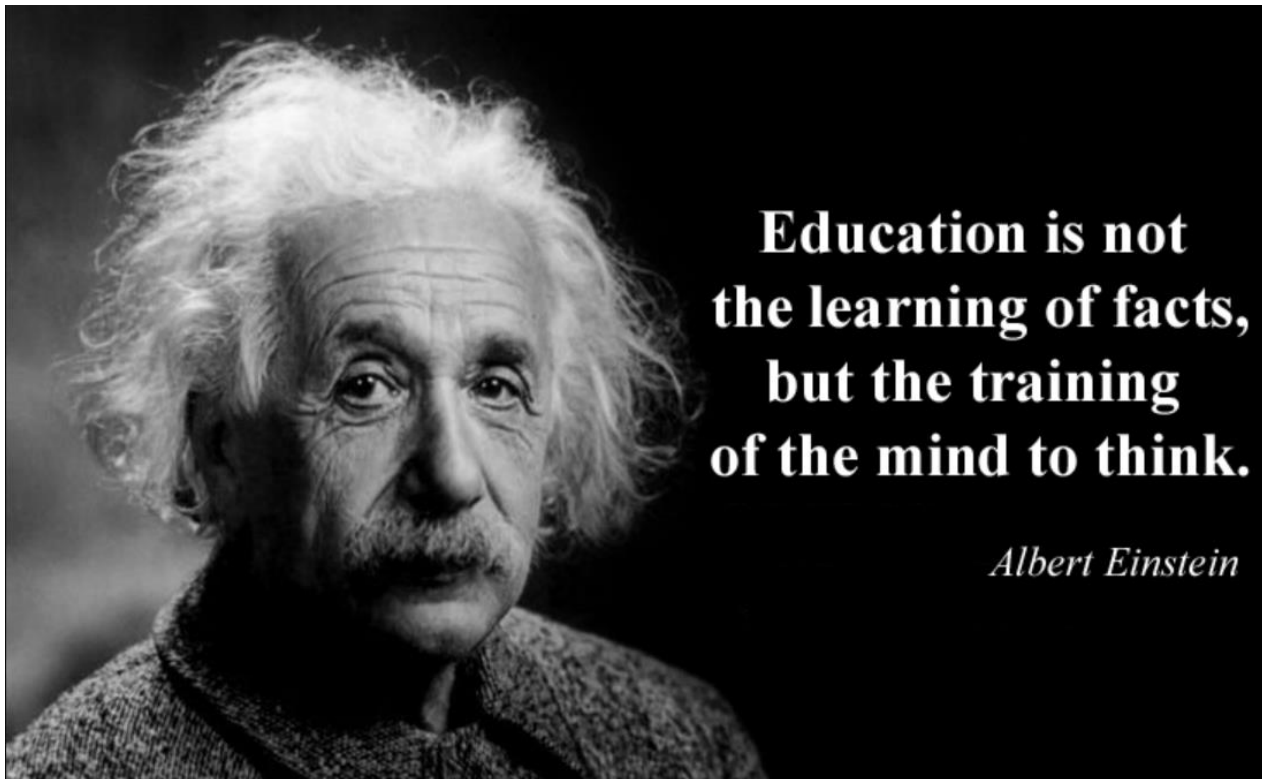
Upsides:

- Everyone can learn at a suitable moment
- Scalability & Consistency
- Reduced Costs
- No need to travel to a classroom
- Audio and video is supported

Downsides

- One-off exercise once every 12, 18 or 24 months
- Content is quickly outdated
- Sequential issues





We need information on everything that involves security risks, e.g.

- Handling confidential information
 - Mobile Device Security
 - Browsing the web
- etc

We opted for Continuous Learning

Learning Goal: **Employees should be able to identify risks in different situations**

Together with our Compliance department we introduced an app called *Sharp*.

- Questions & answers are **randomized**
- Various types of questions
- New content is added **every month**
- Participation is mandatory
- Minimum score of 70%

Fun: People can play duels against each other

Sharp takes each employee 5 minutes per month

Learning Metrics

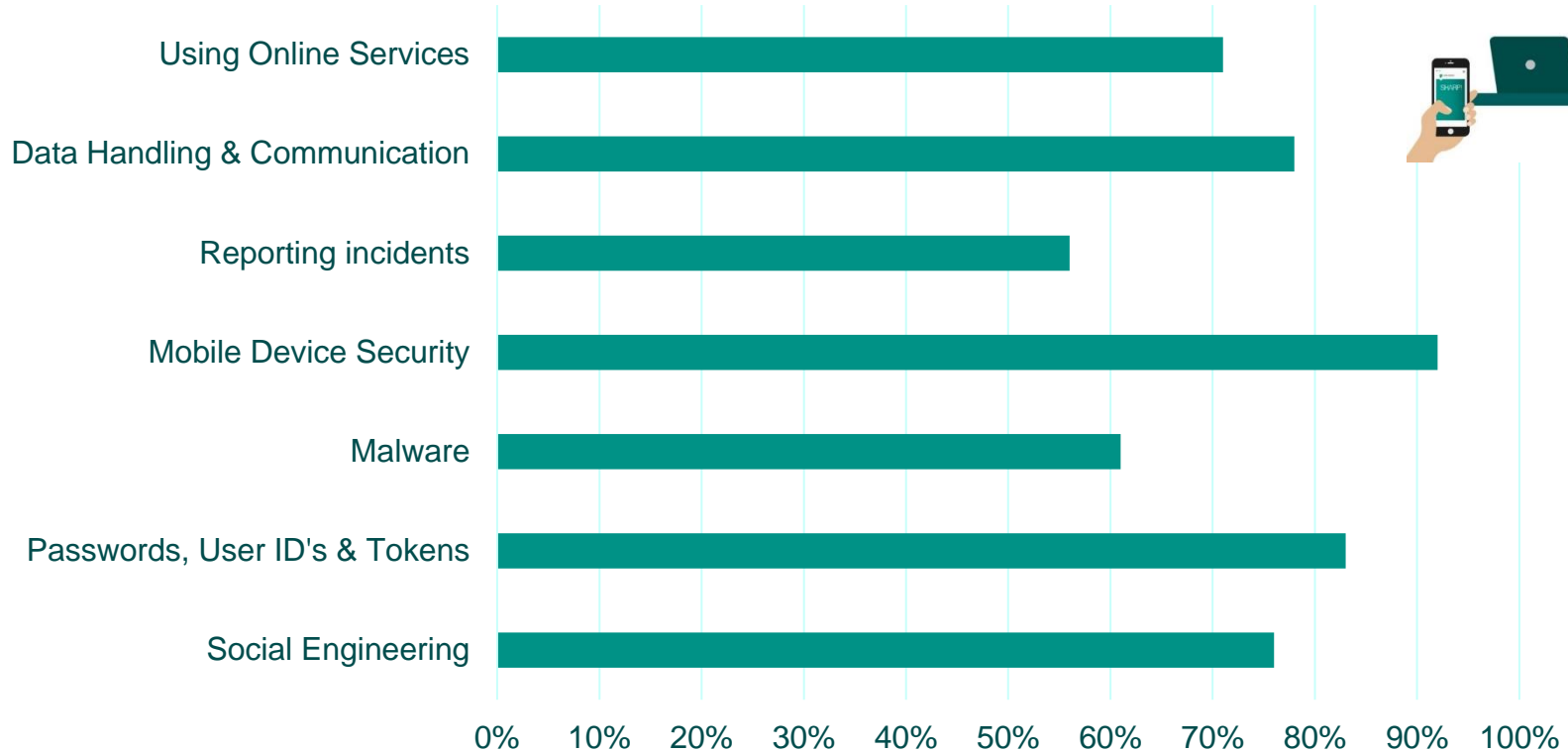
300+ questions divided over buckets (e.g. Malware, Social Engineering, Money Laundering)

Available metrics:

- score per employee
- score per question
- score per bucket
- score per department, business line, country



Thanks to CL we now have detailed metrics



**Education
metrics**



**What about
employee
behaviour?**

How to behave...

Information Security Awareness and Secure Behaviour Policy

But as with many other policies...

Ownership and Classification of Information Assets Policy
Information Security Risk Assessment and Treatment Policy
Information Security Awareness and Secure Behaviour Policy
System Hardening Policy
Information Security Logging and Monitoring Policy
Cryptographic Services Policy
Secure Data Handling Policy
Malware Protection Policy
Identity and Access Policy
Secure System Development and Acquisition Policy
Information Security Incident Management Policy
Etc.



We therefore have rules how to behave

Examples

- Report suspicious emails
- Use unique and strong passwords
- Encrypt confidential data before you send it to external parties
- Lock you laptop when you leave your desk
- Do not email confidential information to your private email address

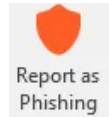
But...



Lesson #1 - Make it as easy as possible...

- Report suspicious emails

>> Phishing button



- Use unique and strong passwords

>> Deploy a password vault



KEEPER

LastPass ****



Keepass

- Encrypt confidential data before you send it to external parties

>> An email encryption button in Outlook would be useful...

Are we there yet?

Knowledge



Opportunity



Motivation

Neutralisation techniques

International studies: People use neutralisation techniques to excuse themselves from having to act in compliance with the rules.

Denial of responsibility

Denial of the victim

Appeal to higher loyalties

Entitlement

Defence by comparison

Denial of injury

Condemnation of the condemner

Defence of necessity

Relative acceptability

Morris & Higgins, 2009; Silic, Barlow, & Back, 2017; Siponen & Vance, 2010; Siponen, Puhakainen, & Vance, 2020. Sykes & Matza, 1957; Collins, 1994; Cromwell & Thurman, 2003; Minor, 1981

How did we measure behaviour?

How did we measure employee behaviour in the past?

- Clean Desk inspections
- Security Incidents, e.g.
 - Lost or stolen devices
 - Malware infections
- People reporting security incidents
- Surveys

But what are we measuring in cyber security surveys?

Behaviour

Phishing email

Malware warning

Password use

Downloading files

Sharing information

Visiting websites

USB stick use

Factors that influence results

Knowledge

Depletion

Usable alternatives

Technical skills

Stress

Default option

Internet use

Habituation

Gamification

Previous victimization

Responsibility / Effect on others

Nudging

Personality

Clear relation cause & effect

Social comparison

Risk perception

Personalize the message

Normative social influence

Demographics

Feeling observed

Security culture

Fair treatment

Remove anonymity

Cost-benefit trade-off

Users

Employees

Security experts

High profile targets

Source: Erasmus University

No more surveys on secure behaviour



Cloud Access Security Broker

What online services are our
employees using?

Example CASB – Videoconferencing services

Name	Category	Name	Category	Name	Category
ClearSea	Online Meetings	Jitsi	Online Meetings, VoIP	Board Management	Online Meetings
Avaya	Collaboration, Online Meetings	ReadyTalk	Online Meetings	BT MeetMe	Online Meetings
24sessions	Online Meetings	Kontiki Software	Online Meetings	TurboBridge	Online Meetings
Adobe Connect	Online Meetings	LiveConf	Online Meetings	MeetingBooster	Online Meetings
GlassFrog	Online Meetings	Macquarie Conferencing	Online Meetings	Zoho Meeting	Online Meetings
BlueJeans	Online Meetings	StartMeeting	Online Meetings	WhyGo	Online Meetings
join.me	Online Meetings	HighFive	Online Meetings	AlignMeeting	Online Meetings
Cisco Webex Teams	Collaboration, Messaging, Meetings	EZTalks	Online Meetings, VoIP	247meeting	Online Meetings
Citrix GotoMeeting	Online Meetings, Screen Sharing	Vidyo	Online Meetings	JetWebinar	Online Meetings
LoopUp	Online Meetings	Wooclap	E-learning, Online Meetings	Groupize	Online Meetings
Citrix GoToWebinar	Online Meetings	MeetingSift	Online Meetings	FreeBusy	Online Meetings
ClickMeeting	Online Meetings	Lucid Meetings	Collaboration, Online Meetings	FirstAgenda	Online Meetings
Polycom	Online Meetings	Liquid Space	Online Meetings	Adigo	Online Meetings
Screen Leap	Online Meetings, Screen Sharing	Confreere	Online Meetings	Veeting Rooms	Online Meetings
Redback Conferencing	Online Meetings	MeetMax	Appointment, Online Meetings	Tixeo	Online Meetings
Level 3 Web Meeting	Online Meetings	Idiligo Inside	Online Meetings	MaestroConference	Online Meetings
appear.in	Collaboration, Online Meetings	Meeting Application	Online Meetings	GoMeetNow	Online Meetings
Impartus	Online Meetings	Roundee	Online Meetings	UniVoIP	Messaging, Online Meetings, VoIP
UberConference	Online Meetings	Voxeet	Online Meetings	Anymeeeting	Online Meetings
InterCall	Collaboration, Online Meetings	PGiConnect	Online Meetings	MeetingBurner	Online Meetings
Fuze Meeting	Online Meetings	Azeus Convene	Online Meetings	Free Conference Calling	Online Meetings
Globalmeet	Online Meetings	newrow_	Online Meetings	AccuConference	Collaboration, Online Meetings
StarLeaf	Online Meetings	Plann3r	Online Meetings	eShare	Collaboration, Online Meetings
Onstream Meetings	Online Meetings	BigMarker	Marketing, Online Meetings	Easymeeting	Online Meetings
Orange Multimedia Conference	Online Meetings	Less Meeting	Online Meetings	Groupboard	Online Diagramming & Meetings
Arkadin	Collaboration, Online Meetings	JiffleNow	Online Meetings	MyOwnConference	Online Meetings
Videxio	Online Meetings	FreeConference	Online Meetings	BoardTRAC	Online Meetings
FreeConfCall	Online Meetings	Powwownow	Online Meetings	Eyeson	Online Meetings
GetMinute	Online Meetings	MeetingKing	Online Meetings, PM	RESULTS	Online Meetings
WebinarJam	Online Meetings	Blizz	Online Meetings	Eventinterface	Online Meetings
8x8	Online Meetings, VoIP	Vast Conference	Online Meetings	Biba	Online Meetings
				Do.com	Online Meetings

Data Loss Prevention

What confidential information are employees sending to external parties?

Confidential emails

- ✓ Portfolio to customer
- ✓ Risk reports to regulator
- ✓ Equity reports to investors
- ✗ Customer analysis reports to external email address
- ✗ Overview with credit card numbers to private email address

Software Asset Management

What software, extensions & plugins
are employees using?

Identification Shadow IT

- Freeware
- Software that requires a business licence
- Software that is no longer supported
 - ⚠ Vulnerabilities are not patched
- Malware / spyware in software and/or browser extensions

Education
metrics ✓

Behaviour? ✓

Vulnerabilities?

Are employees vulnerable for phishing?



Are employees vulnerable for vishing?



Hackers use various emotional stimuli



Curiosity

Did you hear about....?
Your DHL package is on its way...



Fear

Your account will be closed unless...
We have blocked your credit card



Greed

Win a brand new [gadget]... Just enter your name and...
€ 100 is yours if you...

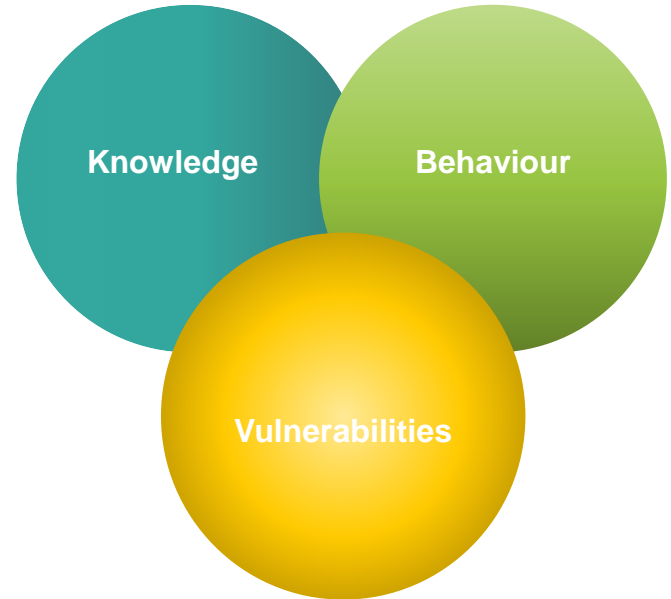


Anxiety

Our CEO just announced that 15% of staff will be laid off
We will publish your private video unless...

Combining all the metrics

- What do people know?
- How do people behave?
- What are their vulnerabilities?



And using the metrics (we're not there yet)

Education

Weak area: social engineering via social media

Behaviour

Uses browser plugins that may contain spyware

Vulnerability areas

Phishing mails triggering fear & anxiety



Martha

HR department

And using the metrics (we're not there yet)

Education

Weak area: regulations & privacy

Behaviour

Downloads Java libraries & JSON formatters

Vulnerability areas

Phishing mails triggering curiosity



Jerry

DevOps

Actions for us to help Martha

- Micro learning on social media abuse
- Wipe plugins & send leaflet on plugins
- Pop-up warnings for incoming emails



This email contains words that are commonly associated with phishing.
Please stay alert!

Actions for us to help Jerry

- Micro learnings on regulation & privacy
- Training on downloading software & other content
- Pop-up warnings for incoming emails



This email contains words that are commonly associated with phishing.
Please stay alert!

- Block services that are labelled dangerous (CASB)
- Escalate serious policy violations to Legal (DLP)
- Enforce data classification
- Remove unlicensed software (SAM)
- Create tailormade pop-up warnings
- Add questions to our Continuous Learning program

- Perform targeted phishing test simulations
- Deliver what is needed where and when it is needed:
 - Assign micro learnings
 - Presentations
 - Posters or Leaflets
 - Play Cyber Attack Simulation game (CybaS)

Goal for 2022

Protect our employees with tailormade awareness interventions and people centric technology

Takeaways

- Replace your annual e-learning with a continuous learning program
- Get metrics on behaviour via tools like CASB, DLP and Software Asset Management
- Analyse usage of online services, shadow IT and monitor email communication
- Perform phishing tests and use real life scams as examples



Thank you for your attention!