A new awareness approach

No more hiding

SANS Awareness Summit – London
November 2019

Version 1.1.
ABN AMRO is a bank that services clients in the retail, private and corporate banking sectors. We offer a comprehensive range of financial products and services across a variety of channels.

Head office is in Amsterdam. The origins go back 300 years.

Sustainability and inclusion are high on the agenda.

Richard Verbrugge
Part of the CISO team
Responsibility: Awareness & Education
A fact we all know too well

We cannot secure behaviour, so our employees have to behave securely.
People are different.

**Challenge:**
Replace the *one size fits all* approach by a people centric approach
Problem:
What do employees know about Information Security and how do they behave now?
In the past we used e-learnings
We learned from the brightest…

_Education is not the learning of facts, but the training of the mind to think._

*Albert Einstein*
We need metrics on each behaviour that involves security risks

- Dealing with passwords
- Handling confidential information
  - Social Engineering
  - Et cetera
Now we have detailed metrics

- Internet & Social Media
- Data Handling & Communication
- Reporting incidents
- Working outside the office
- Malware
- Passwords, User ID's & Tokens
- Social Engineering

Buckets
Education metrics

What about employee behaviour?
How did we measure employee behaviour in the past?

- Clean Desk inspections
- Security Incidents
  - # Lost or stolen devices, files
  - # Infections
- People reporting security incidents & suspicious behaviour
- Surveys
CASB

What online services are our employees using?
Data Loss Prevention

What confidential information are employees sending to external parties?
Snow

What software and plugins are employees using?
Metrics from Phishing tests
Metrics beyond the links and attachments
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
Curiosity & anxiety
• Micro learning on social media abuse
• Questions in CL program
• Wipe plugins & send leaflet on plugins
• Pop-up screens when incoming emails contain keywords associated with curiosity or anxiety
• Block services that are labelled dangerous (CASB)
• Escalate serious policy violations to Legal (DLP)
• Enforce data classification
• Remove unlicensed software (SNOW)
• Create tailormade pop-up warnings
• Add questions to Continuous Learning program
• Perform targeted phishing test simulations
• Deliver what is needed where it is needed:
  • Assign micro learnings
  • Presentations
  • Narrow Casting / Posters / Leaflets
  • Play Cyber Attack Simulation game (CybaS)
Goal for 2021

Protect our employees with tailormade awareness interventions and people centric technology
Takeaways

• Replace long e-learnings with a continuous learning program

• Use tools that measure user behaviour

• Find out what emotions trigger your colleagues

• Drop *the one size fits all* approach and go for a people centric approach
Thank you for your attention!