Kaspersky Lab

Kaspersky cyber safety management game
Healthcare | Bank | Retail scenario

Background / Problem statement:

All organizations are taking steps to address cyberthreats by setting up IT security structures and training compliance. But is this enough?

- Does knowledge gained at training really drive employees' behavior? Or is it something else?
- Does business efficiency have to be sacrificed to achieve security?
- Do security officers feel that there are too few of them to reach every ear in their fight for cyber safety?

These challenges can only be addressed by engaging line managers in making organizations cyber secure, without sacrificing efficiency. Only they interact with employees on a daily basis and make business decisions. The answer lies in making cyber-safety the mandatory ingredient of everyday decision-making. Normally, this is the biggest challenge for the Security team – how to engage management. That's why Kaspersky Lab developed a special training program aimed at converting line/ middle managers into cybersecurity supporters and advocates.

Task:

Create a scenario for Kaspersky cyber safety management game in one of the following areas:

- Healthcare
- Banking sphere
- Retail

Solution requirements:

Choose the industry: Healthcare, Bank or Retail.

1) Create a typical environment with workplaces.
2) Figure out operations people are to perform to achieve their business tasks that may be not secure.
3) Describe typical mistakes people make and possible consequences.
4) Find examples from the internet of cyber security incidents happened in similar situation and attach them to the zone.

Technical requirements for the solution:

1) Comics-like gameboard with 12 zones (PDF file). When printed at A1 should be easily read. Recommendation: avoid massive texts. Sketches are also acceptable.
2) Presentation with 2-6 slides for each zone that describe the threat and provides useful instructions to the user (like in given examples). Links to the related cases are welcome

Evaluation criteria:

- Criterion: Vividness of proposed physical and IT structure
  Evaluation: maximum 5 - minimum 1.
- Variety of threats
  Evaluation: maximum 5 - minimum 1.
- Reliance on real cases
  Evaluation: maximum 5 - minimum 1.
- Quality of elaboration
  Evaluation: maximum 5 - minimum 1.

Study materials:

https://box.kaspersky.com/f/e026caa9df0a49d8bfdf/