

Designing with Cyber Security in mind

Ronald Osure

KENET Cyber Security Training
October 26th - 30th 2015

Agenda

- Staying ahead in the cyber security game
- Security center stage
- Security is already created or lost at the design stage
- Persuasive technologies
- Fear as a tool

“We don't care how it works, as long
as it works”

Staying ahead in the cyber security game

What matters now

Cyber security is a field in motion, perhaps
even more that IT itself

Can we trust the system?

The internet was never designed with security
in mind

Can we make the organizations more secure?

The next level down is about creating a secure organization that can survive and thrive in the midst of imperfect technologies.

Can our people win the game?

Right now, the reality is that sophisticated attackers are breaking through conventional safeguards every day

What will technology bring next?

In one study, 70% of security executives expressed concern about cloud and mobile security

Security centre stage

How the continuing battle between the “good guys” and the “bad guys” is ultimately making the world more secure

Where would the world be without
Internet?

Privacy & Security – Two sides of the same medal

- Big data, social media and increased availability of location data
 - Who owns data?
- Emerging concepts surrounding data ownership
- Privacy and Security extend organizational boundaries

Impact of cyber security – Does it matter?

In the end how does all this affect organizations?

A wishlist for cyber security

“What should be the most important advances in security on the coming few years?”

- Better solutions for securing end to end communication
 - Know who's connected – 100% certainty
 - Use secure applications over insecure infrastructure
 - Increased role for biometrics



A wishlist for cyber security

- Smart systems
 - Self-learning security system
 - Auto classification of data
- A better way to communicate to users about security
 - Framework for security warnings
 - Label showing level of security (certified) on apps

What good will come from all this?

Security is already created or lost
at the design stage

If only we could re-design everything from
the start

What is recent?

- Software development has professionalized dramatically
- Big transformation in IT with the introduction of Cloud

Why is this relevant?

Security-by-design is one of the powerful approaches we have available to make everything more secure

What action should I take?

- Make security part of the enterprise architecture discussion
- Create anti-patterns
- Put enough time and budget into projects

“Security must be at the heart of systems, with Trusted Computing. There is a great need to build secure applications within an infrastructure that is not! We will never secure the entire chain. Security should be first in the planning of the projects, before thinking of the rest. More often it happens the other way around.”

– cso of a research institute

The key to security is implementing
persuasive technologies

“Choose a password of at least 12 characters that include capital letters, special characters and that does not contain any regular names or words. Oh, and don't write it down.”

What is recent?

Users have the power to circumvent

Why is this relevant?

If we can create the right circumstances,
we can make the user an enormous force
for good

Actions that can be taken

- Rethink organizational processes with security in mind
- Give people small “rewards” for doing the right thing
- Provide technical tools to make it easy
- Make insecure things hard
-

Fear as a tool is going blunt very
rapidly

From Fear to Value

Make “**Being Secure**” part of your core values

References

- Staying ahead in the Cyber Security Game
 - Erik van Ommeren
 - Martin Borrett
 - Marinus Kuivenhoven