Investing in Security

Claudiu Constantinescu, CISA
Former OWASP Chapter Leader
S&T Romania

05.06.2013

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.
What is Security?

- Security in general is...

  *Confidentiality, Integrity, Availability*

- Information security is commonly understood as...

  *practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.*
## Timeline

<table>
<thead>
<tr>
<th>Area</th>
<th>‘80s</th>
<th>‘90s – early 2000s</th>
<th>Late 2000s+</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Investment</td>
<td>Technology (mainframes)</td>
<td>Technology and solutions</td>
<td>Business Driven</td>
</tr>
<tr>
<td>Security threats</td>
<td>Non-threatening</td>
<td>Sporadic/ fame based</td>
<td>Targeted attacks APTs Monetized</td>
</tr>
<tr>
<td>Security responsibility</td>
<td>IT</td>
<td>Within IT</td>
<td>Dedicated (CISO)</td>
</tr>
<tr>
<td>Security solutions</td>
<td>Firewalls</td>
<td>Embedded in IT systems + punctual</td>
<td>Everything possible and still developing</td>
</tr>
<tr>
<td>Security investments</td>
<td>N/A</td>
<td>FUD-driven</td>
<td>Anything goes 😊</td>
</tr>
</tbody>
</table>
Risk Management

- Exposure / Vulnerability
  - *How much am I to lose?*

- Probability / Threat
  - How often do I lose?

- In theory
  - loss expectancy = exposure x probability
  - Risk = vulnerability x threat (or almost)

- In practice
  - Impossible to quantify

- Never invest in security more than the asset you are protecting is worth – *but how much do I really stand to lose?*
Attitude

- Business wants traditional ROI model – security does not fit
  "when will I get my investment back?"
  "hopefully never"

- IT
  - Not a problem, everything is OK

- Dedicated security (CISO)
  - It is far worse than you imagine (FUD)

- Business management
  - I invest a little bit, maybe I will invest some more in the future, but
    hopefully nothing bad happens meanwhile (/pray 😊)

- Facing a security event
  - Why did it happen to me??

- Balanced risk management? Anyone?
Kübler-Ross model (developed for hospital patients facing impending death)

- Denial — "I feel fine."; "This can't be happening, not to me."
- Anger — "Why me? It's not fair!"; "How can this happen to me?"; "Who is to blame?"
- Bargaining — "I'll do anything for a few more years."; "I will give my life savings if..."
- Depression — "I'm so sad, why bother with anything?"
- Acceptance
Key drivers in security investment

- Reported (PwC report 2013)
  - Economic conditions
  - Business continuity / disaster recovery
  - Company reputation
  - Change and business transformation
  - Internal policy compliance
  - Regulatory compliance

- Others (and *very* subjective)
  - Fear, uncertainty and doubt (still)
  - Political power (“I build for this company”)
  - Control over personnel
  - Misunderstanding of risks

- Key issues in security spending (subjective, too)
  - Ignoring problems (do not spend)
  - Misunderstanding of limitations (false sense of security)
  - Not directly tackling exposure
Thank you!

*These views are my own. Not OWASP’s, employer’s, parents, educators, etc.*