The Impact of Software Security Practices on Development Effort

Elaine Venson and Barry Boehm
USC Center for Systems and Software Engineering

Research Task / Overview

- The **effort/costs** of performing security practices are often pointed out as a barrier to their wide use.
- **Lack of knowledge** about the amount of resources needed to achieve a determined level of security assurance.
- It is paramount for users, developers and managers to **understand and agree** on the right amount of resources to be allocated for software projects to deliver proper security.

Goals & Objectives

- Gather a better understating of how software security practices are applied in the industry:
  - Effort and frequency of activities.
- Identify the implications of applying such activities in terms of effort:
  - Effort added in projects.
  - Effort estimation methods.

Data & Analysis

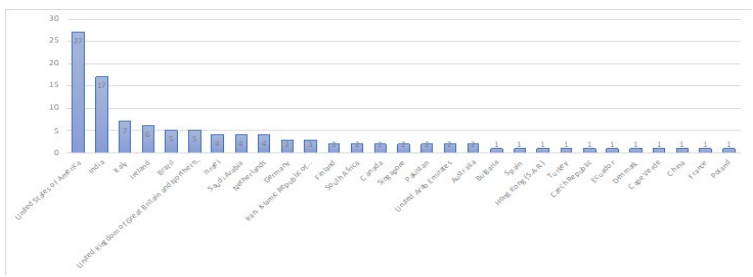
110 complete responses

13.61% of the sample

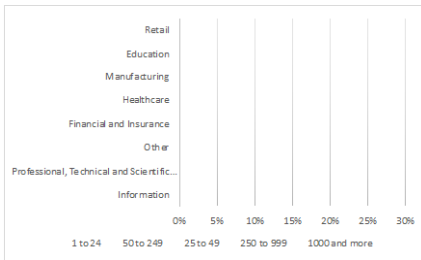
Confidence Interval 9.07

Level of Confidence 95%

Participants per Country



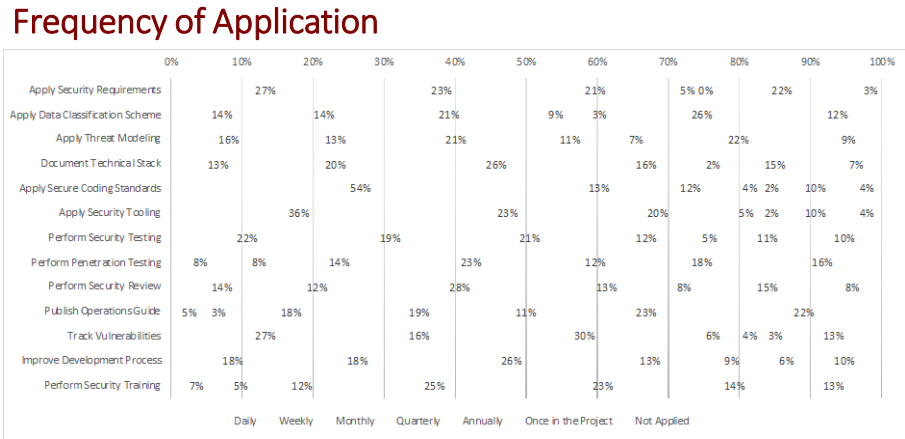
Organization Size and Domain



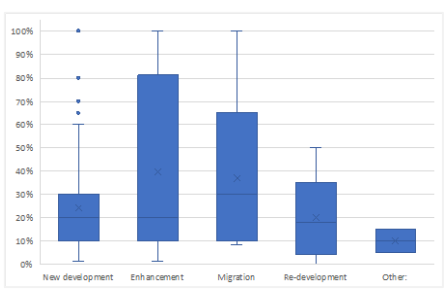
Selected Project

	Team Size	Duration (months)	Project Size (PM)	Security Risk Level
Min	1.0	0.5	4.0	1.0
1st Qu.	5.0	6.0	30.0	3.0
Median	8.0	11.0	85.0	4.0
Mean	33.2	14.3	564.3	3.7
3rd Qu.	20.0	15.8	366.0	5.0
Max	1000.0	97.0	12000.0	5.0
Std. Dev.	108.7	14.6	1785.9	1.3
NA	13.0	14.0	14.0	16.0

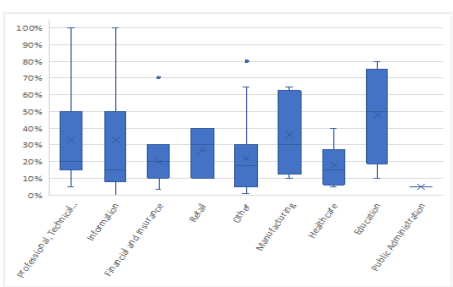
Frequency of Application



Effort Dedicated to Security



By Development Type



By Sector

Estimation Methods and Use

Method / Planning	Yes	Part	No	NP	Ov(n)	Ov(%)
Analogy Based	5	5	1	0	11	11.3%
Expert judgment	27	14	3	1	45	46.4%
Function Point Based	3	2	0	1	6	6.2%
Parametric model	1	1	0	0	2	2.1%
Work breakdown	15	4	2	0	21	21.6%
Not known	2	5	0	1	8	8.2%
Other	2	2	0	0	4	4.1%
Overall (n)	55	33	6	3	97	100.0%
Overall (%)	57%	34%	6%	3%	100%	

Methodology

Sampling Frame

- *Software Security Group on LinkedIn*
- 2012 member at the time

Sampling Strategy

- *Random Sampling*
- *Initial sample size = 908*
- *Excluding recruiters and sales people = 808*

Recruitment Strategy

- *Manual invitation through LinkedIn messages*
- *Raffle on Amazon to encourage responses*

Questionnaire Design

- *Reviewed by external expert*
- *Piloted with 10 members from the sampling frame*
- *Close-ended and quantitative questions*
- *One open-ended question*

Data Collection and Analysis

- *Web-based tool*
- *Available for 2 weeks*
- *Reminder after 1 week*
- *Quantitative analysis mostly*

Future Research

- Identify the degrees of application of security practices and security requirements in software development.
- Understand the variation of other cost factors when the security factor is included in effort estimation models.
- Compare the increase pattern of development effort with increased levels of security implemented.
- Elaborate a model to explain the increase in development effort caused by the degree of required security.

Contacts/References

Elaine Venson: venson@usc.edu
Barry Boehm: boehm@usc.edu

Elaine Venson, Reem Alfayez, Marília M. F. Gomes, Rejane M. C. Figueiredo, and Barry Boehm, "The Impact of Software Security Practices on Development Effort: An Initial Survey," in *Proceedings of the 13th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, New York, NY, USA, 2019.