Pilots, Surgeons and Developers

Improving Application Security With Checklists

OWASP Global AppSec D.C. 2019 - Joe Kuemerle / @jkuemerle

https://www.flickr.com/photos/28476480@N04/3931491307

https://www.flickr.com/photos/57763385@N03/11354819183

https://www.flickr.com/photos/82993642@N03/7642566946

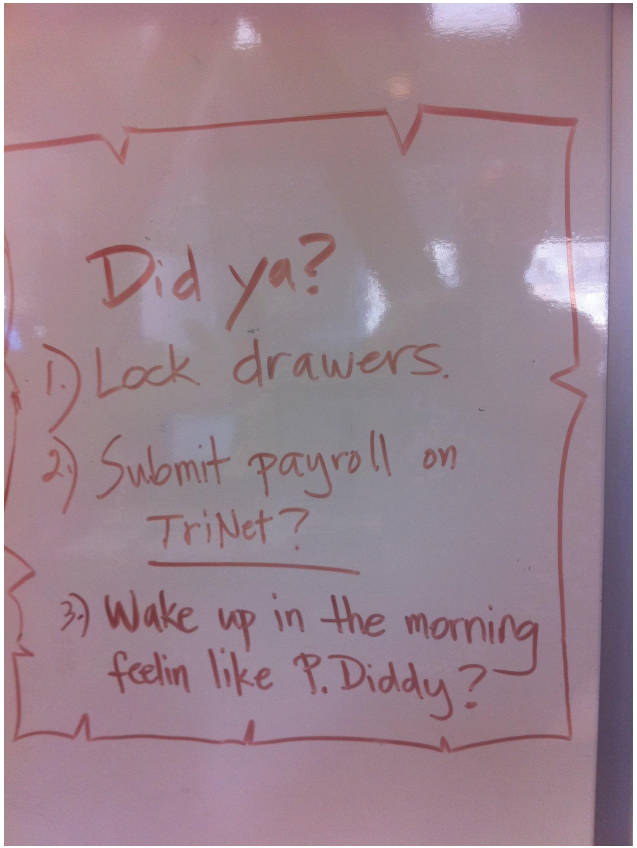
- ★ Product Security Engineer @ Salesforce
- ★ Technical Speaker
- ★ Developer, data integration, analytics and development processes
- ★ Techbash Conference
- ★ Potions professor
- ★ @jkuemerle / www.kuemerle.com

“ ...the volume of what we know has exceeded our individual ability to deliver its benefits correctly, safely, or reliably. Knowledge has both saved us and burdened us.

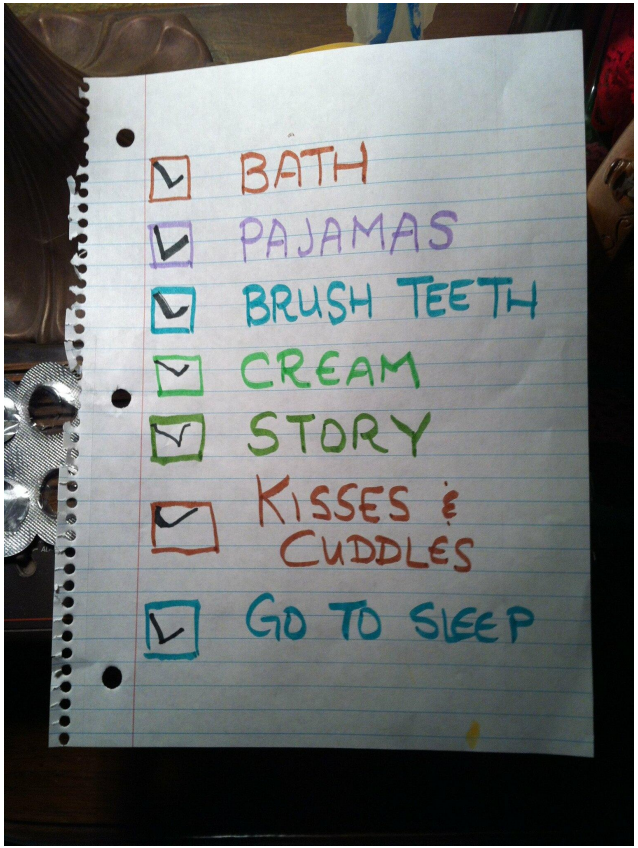
That means that we need a different strategy for overcoming failure, one that builds on experience and takes advantage of the knowledge people have but somehow also makes up for our inevitable human inadequacies. And there is such a strategy - though it will seem almost ridiculous in its simplicity, maybe even crazy to those of us who have spent years carefully developing ever more advanced skills and technologies.

It is a checklist.”

Atul Gwande - The Checklist Manifesto



https://www.flickr.com/photos/89306448@N00/5331464979



https://www.flickr.com/photos/30963564@N00/8443668738

https://www.flickr.com/photos/65097875@N07/7381685460

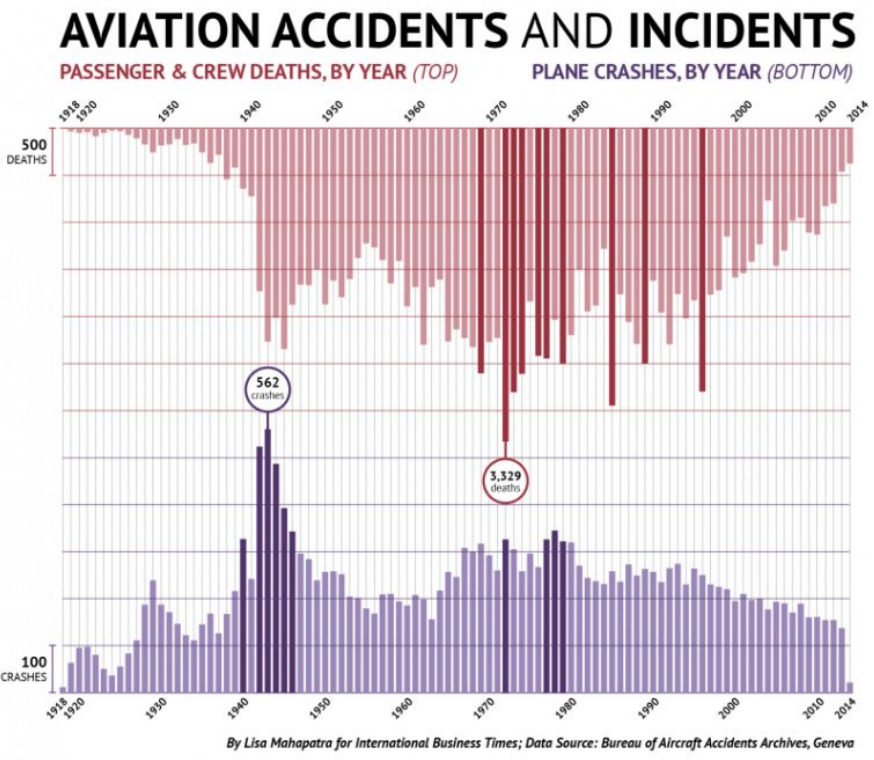
@jkuemerle

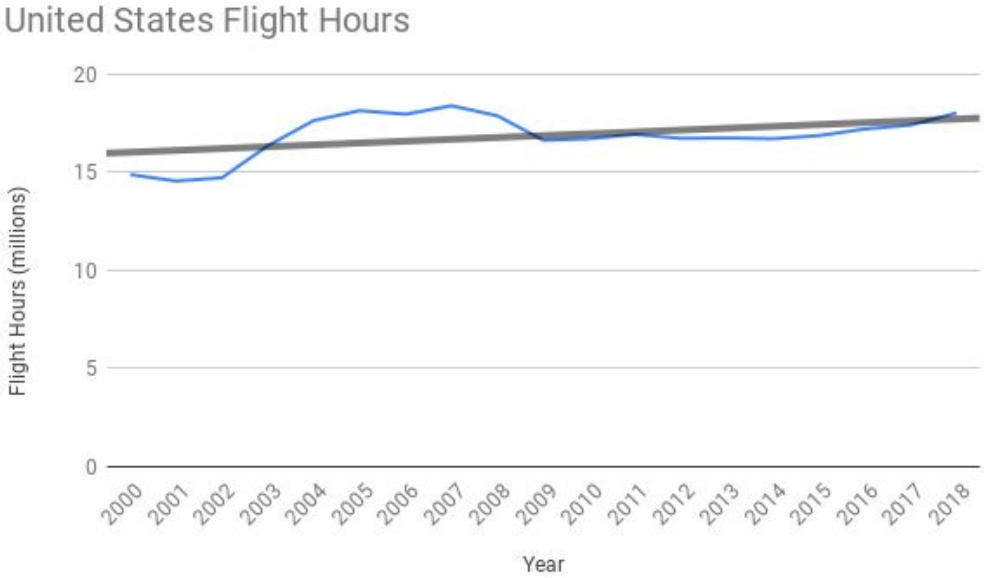
https://upload.wikimedia.org/wikipedia/commons/b/b1/Harry_Potter_1st_USA_ed._complete_hardback_set_stacked_with_ruler_horizontal.JPG

@jkuemerle

https://www.flickr.com/photos/45394900@N00/2812395984

@jkuemerle





https://www.transtats.bts.gov/TRAFFIC/

Lessons We Can Learn From Aviation Checklists

https://blog.safetyculture.com/checklist-best-practices/lessons-we-can-learn-from-aviation-checklists

“Use of the WHO Surgery Checklist reduced the rate of deaths and surgical complications by more than one-third across all eight pilot hospitals.

The rate of major inpatient complications dropped from 11% to 7%, and the inpatient death rate following major operations fell from 1.5% to 0.8%.”

A surgical safety checklist to reduce morbidity and mortality in a global population

New England Journal of Medicine 2009

Surgical Safety Checklist

World Health Organization | Patient Safety
A World Alliance for Safer Health Care

Before induction of anaesthesia

(with at least nurse and anaesthetist)

Has the patient confirmed his/her identity, site, procedure, and consent?
- ☐ Yes

Is the site marked?
- ☐ Yes
- ☐ Not applicable

Is the anaesthesia machine and medication check complete?
- ☐ Yes

Is the pulse oximeter on the patient and functioning?
- ☐ Yes

Does the patient have a:

Known allergy?
- ☐ No
- ☐ Yes

Difficult airway or aspiration risk?
- ☐ No
- ☐ Yes, and equipment/assistance available

Risk of >500ml blood loss (7ml/kg in children)?
- ☐ No
- ☐ Yes, and two IVs/central access and fluids planned

Before skin incision

(with nurse, anaesthetist and surgeon)

- ☐ **Confirm all team members have introduced themselves by name and role.**
- ☐ **Confirm the patient's name, procedure, and where the incision will be made.**

Has antibiotic prophylaxis been given within the last 60 minutes?
- ☐ Yes
- ☐ Not applicable

Anticipated Critical Events

To Surgeon:
- ☐ What are the critical or non-routine steps?
- ☐ How long will the case take?
- ☐ What is the anticipated blood loss?

To Anaesthetist:
- ☐ Are there any patient-specific concerns?

To Nursing Team:
- ☐ Has sterility (including indicator results) been confirmed?
- ☐ Are there equipment issues or any concerns?

Is essential imaging displayed?
- ☐ Yes
- ☐ Not applicable

Before patient leaves operating room

(with nurse, anaesthetist and surgeon)

Nurse Verbally Confirms:
- ☐ The name of the procedure
- ☐ Completion of instrument, sponge and needle counts
- ☐ Specimen labelling (read specimen labels aloud, including patient name)
- ☐ Whether there are any equipment problems to be addressed

To Surgeon, Anaesthetist and Nurse:
- ☐ What are the key concerns for recovery and management of this patient?

This checklist is not intended to be comprehensive. Additions and modifications to fit local practice are encouraged.

Revised 1 / 2009

© WHO, 2009

https://apps.who.int/iris/bitstream/handle/10665/44186/9789241598590_eng_Checklist.pdf

@jkuemerle

https://www.flickr.com/photos/21597369@N06/2091577071

https://www.flickr.com/photos/81434653@N00/4597488208

“We believe that normal checklists are intended to achieve the following objectives:

1. Provide a standard foundation for verifying aircraft configuration that will attempt to defeat any reduction in the flight crew's psychological and physical condition.
2. Provide a sequential framework to meet internal and external cockpit operational requirements.
3. Allow mutual supervision (cross checking) among crew members.
4. Dictate the duties of each crew member in order to facilitate optimum crew coordination as well as logical distribution of cockpit workload.
5. Enhance a team concept for configuring the plane by keeping all crew members “in the loop.”
6. Serve as a quality control tool by flight management and government regulators over the flight crews.

Another objective of an effective checklist, often overlooked, is the promotion of a positive “attitude” toward the use of this procedure. For this to occur, the checklist must be well grounded within the “present day” operational environment, so that the flight crews will have a sound realization of its importance, and not regard it as a nuisance task (Nagano, 1975). ”

Cockpit Checklists: Concepts, Design, and Use
https://ti.arc.nasa.gov/m/profile/adegani/Cockpit%20Checklists.pdf

https://www.flickr.com/photos/30490214@N03/37781180025

https://www.flickr.com/photos/33104187@N04/28669836291

@jkuemerle

https://www.flickr.com/photos/58611670@N04/12034754536

https://www.flickr.com/photos/34534185@N00/6052621788

https://www.flickr.com/photos/33104187@N04/19405783446

@jkuemerle

https://www.flickr.com/photos/33104187@N04/9294538702

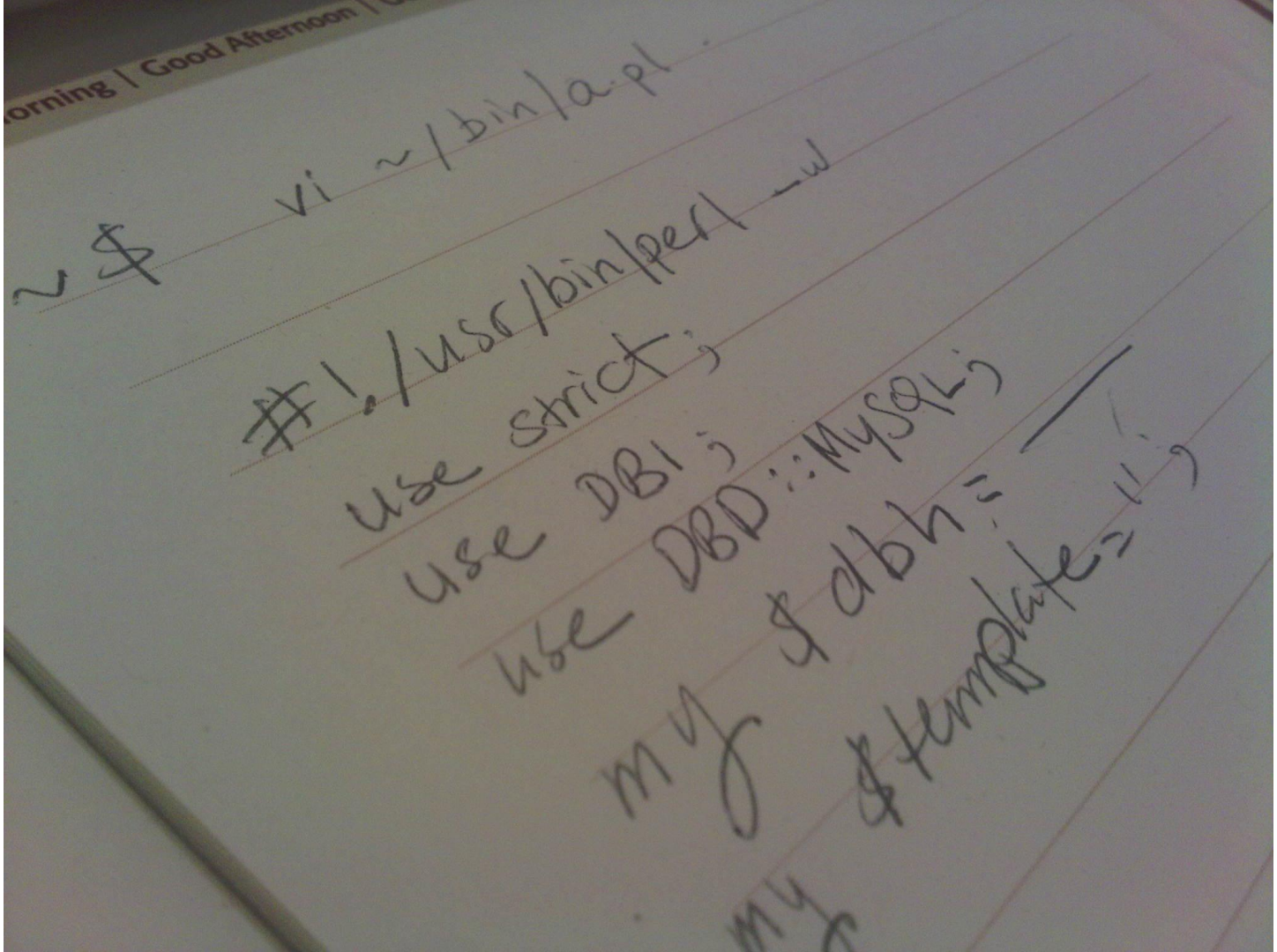
@jkuemmerle

“The various ways of conducting a checklist are influenced not only by the checklist device and the method of using it, but also by its “philosophy of use.” This philosophy varies among airframe manufacturers, officials of regulatory agencies, and airlines. In most cases, the checklist philosophy of use is the outgrowth of the company’s corporate culture.

…

The airline’s culture is an important factor because it is mirrored in the manner in which flight management and training departments establish, direct, and oversee flight operations and related procedures (Degani and Wiener, 1991). ”

Cockpit Checklists: Concepts, Design, and Use
https://ti.arc.nasa.gov/m/profile/adegani/Cockpit%20Checklists.pdf



https://www.flickr.com/photos/9461373@N05/5472232343

@jkuemerle

https://www.flickr.com/photos/37996646802@N01/33471651681

https://www.flickr.com/photos/77846644@N00/112869208

@jkuemerle

“Management pressure for “on-time performance” is one factor that yields high operating efficiency. Air transports fly in and out of hubs with fast turnarounds. The Department of Transportation monitors flight schedules in order to publish the highest and lowest ranking airlines in “on-time performance,” placing another public relations burden on management. Such production pressures ultimately migrate into the cockpit, and consequently affect checklist management.

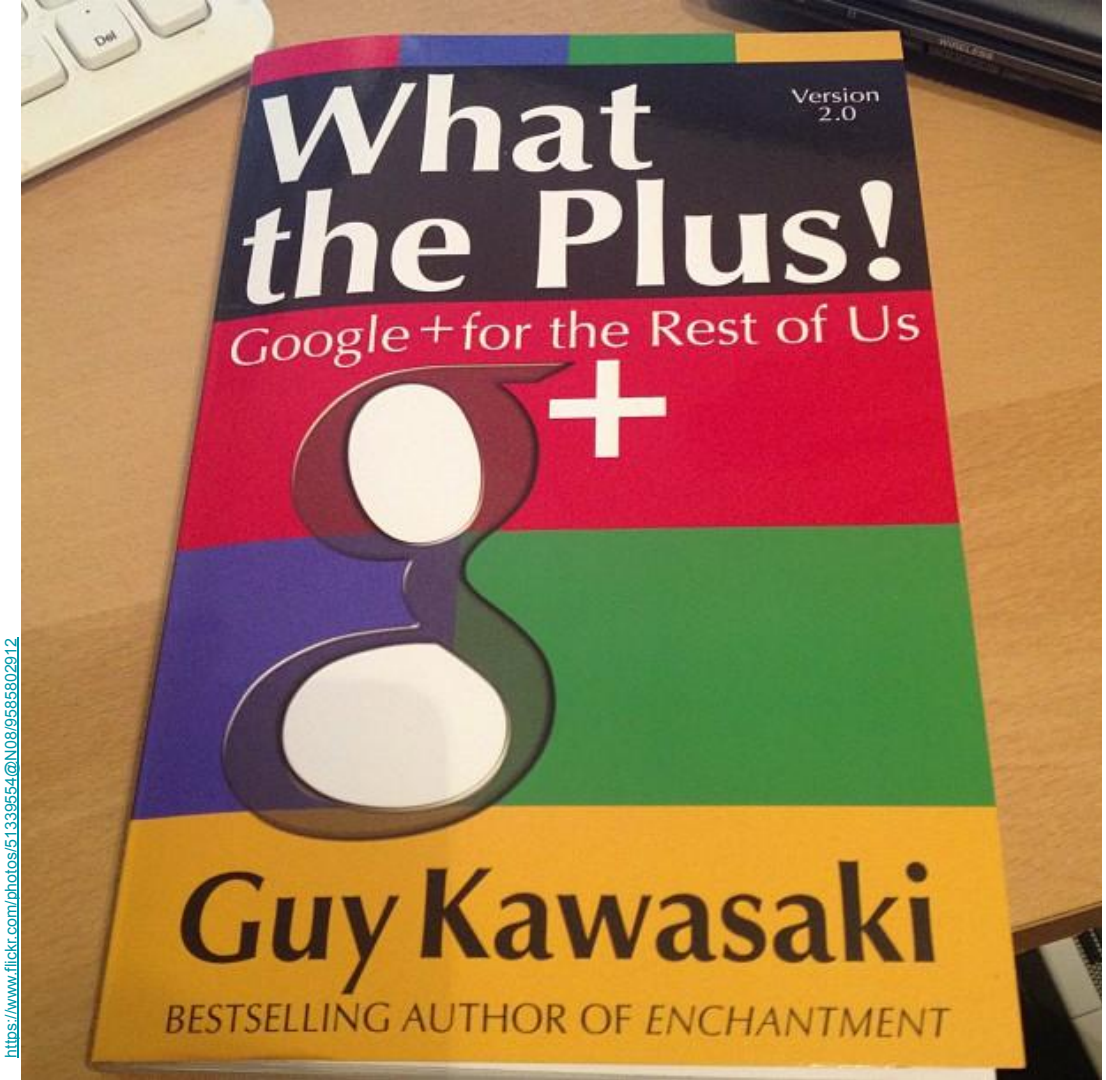
The checklist procedure is highly susceptible to production pressures. These pressures lay the foundation for errors by encouraging sub-standard performance when the crew is rushing to complete the checklist in order to depart on time. Furthermore, under production pressures, checklists are sometimes “...relegated to second place status in order to save time” (Majikas, 1989). ”

Cockpit Checklists: Concepts, Design, and Use
https://ti.arc.nasa.gov/m/profile/adegani/Cockpit%20Checklists.pdf

https://www.flickr.com/photos/37914686@N00/2928818748

@jkuemerle

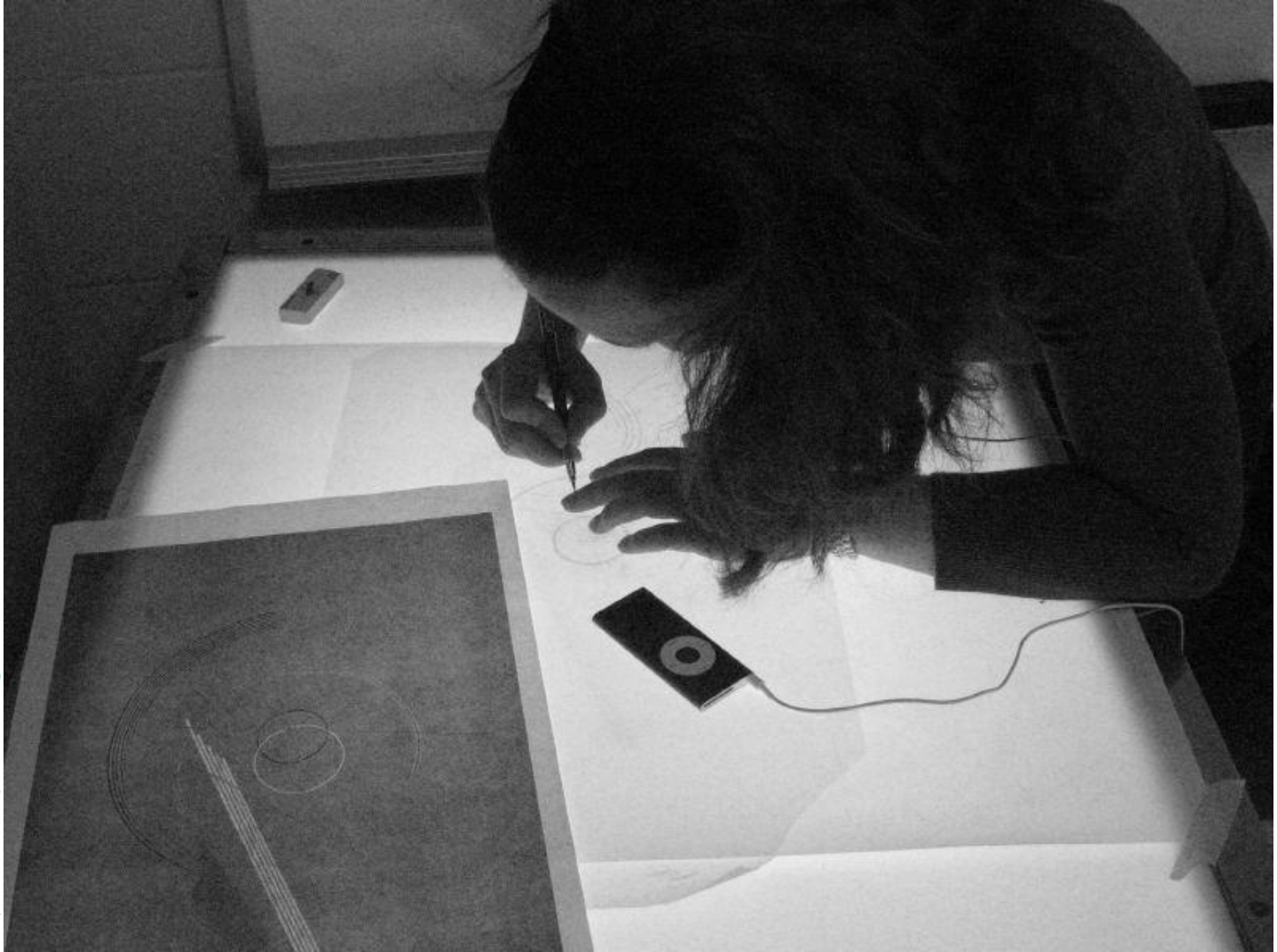
https://www.flickr.com/photos/84987970@N00/8736519237



https://www.flickr.com/photos/51339554@N08/9585802912

https://www.flickr.com/photos/43998657@N02/18526571462

@jkuemerle



https://www.flickr.com/photos/58919362@N00/1440580996

@jkuemerle

https://www.flickr.com/photos/97587214@N00/1185702926

@jkuemerle

Bill Sempf
@sempf

Following

QA Engineer walks into a bar. Orders a beer. Orders 0 beers. Orders 999999999 beers. Orders a lizard. Orders -1 beers. Orders a sfdeljknesv.

1:56 PM - 23 Sep 2014

https://twitter.com/sempf/status/514473420277694465

https://www.flickr.com/photos/68877611@N00/5447032661

https://www.flickr.com/photos/26747023@N00/346073366

@jkuemerle

Am I allowing the user to change the value of stored data?

☐ No

☐ Yes, and I am making sure the user is both identified and is authorized to make the requested changes

Am I exposing an internal identifier value to the user?

☐ No

☐ Yes, and I am making sure the user is both identified and is authorized to view or work with the item

Am I returning any values that the user entered back to the user?

☐ No

☐ Yes, and I am making sure the values are escaped for the rendering context

Am I processing any user provided XML data?

☐ No

☐ Yes, and I am using an XML parser that is configured to reject embedded document type declarations (DTD)

1. **Checklist responses should portray the desired status or the value of the item being considered, not just “checked” or “done.”**

☐ Items all have status indicating desired value

2. **A long checklist should be subdivided to smaller task-checklists or chunks that can be associated with systems and functional areas.**

☐ Checklist is subdivded according to task specific areas

3. **Sequencing of checklist items should follow a meaningful organization of the tasks, and be performed in a logical flow.**

☐ Checklist items are in a logical order

4. **Checklist items should be sequenced in parallel with internal and external activities that require input from other parties (operations, project/product management, stakeholders)**

☐ Items that require external input are in parallel

5. **The most critical items on the task-checklist should be listed as close as possible to the beginning, in order to increase the likelihood of completing the item before interruptions may occur. This could conflict with No. 4 above. In most cases where this occurs, this guideline should take precedence.**

☐ Critical items are listed as close as possible to the top

6. **Critical checklist items that need to be reevaluated due to new information, should be duplicated in checklists for the appropriate situation (testing, runtime, etc.).**

☐ Items requiring reevaluation are duplicated where appropriate

7. **The completion call of a checklist should be written as the last item on the checklist, allowing team members to move mentally from the checklist to other activities with assurance that the checklist has been completed.**

☐ Checklist ends with a completion task

8. **Critical checklists should be completed early in the process in order to decouple them from the other activities that may cause distraction.**

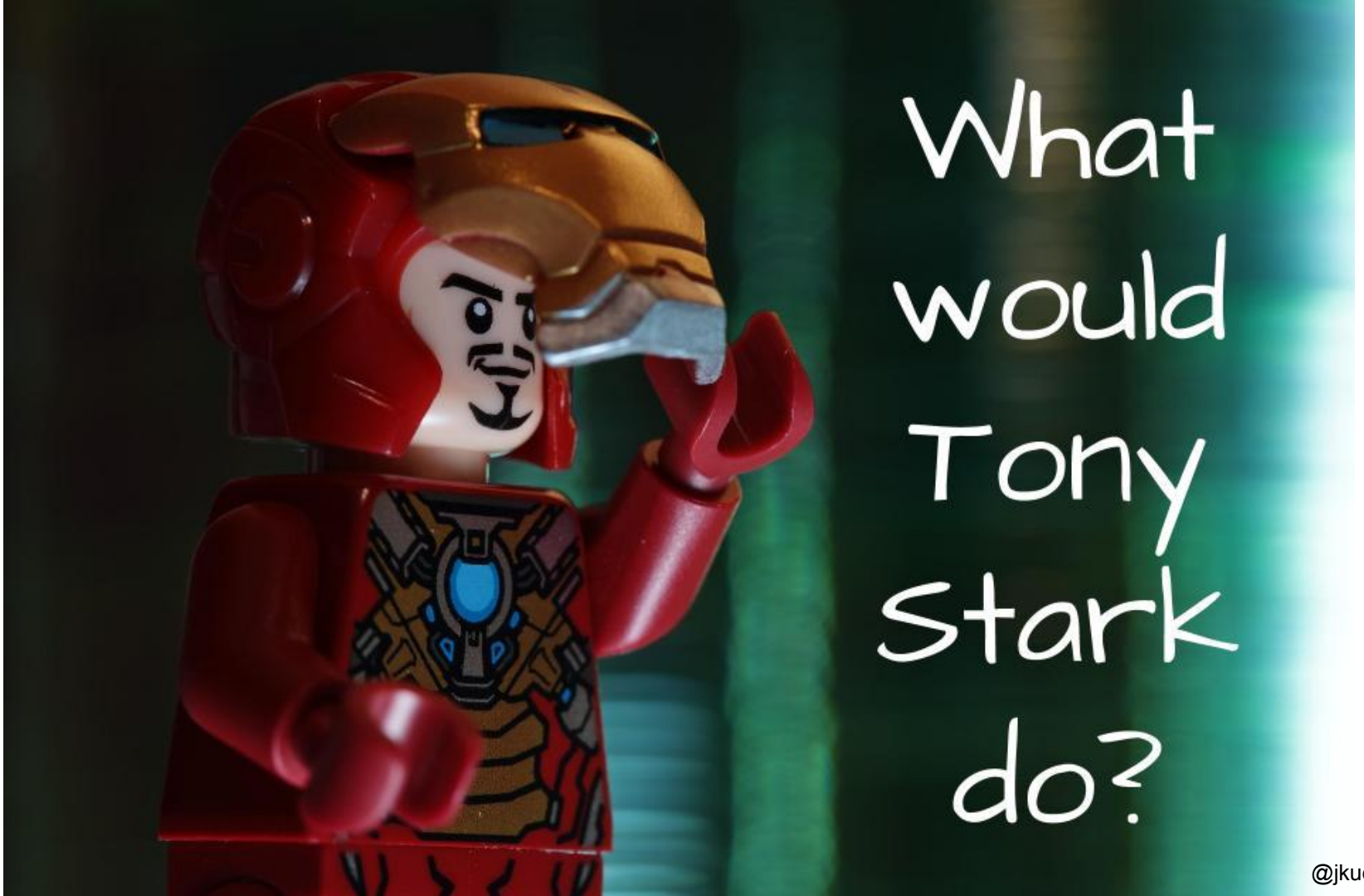
☐ Critical checklist is documented to be completed first

9. **Checklists should be designed in such a way that their execution is not tightly coupled with other tasks. Provide buffers for recovery from failure and a way to “take up the slack” if checklist completion does not keep pace with other activities.**

☐ Checklists do not have tightly coupled tasks

10. **Teams should be aware that checklist procedure is highly susceptible to production pressures. These pressures set the stage for errors by possibly encouraging substandard performance, and may lead some to relegate checklist procedures to a second level of importance, or not use them at all.**

☐ Development has a sense of ownership of checklists



https://www.flickr.com/photos/113562593@N07/15908417404

@jkuemerle

References

- The Checklist Manifesto - Atul Gawande http://bit.ly/ChecklistManifestoOWASP
- Hidden Brain Podcast: You 2.0: Check Yourself http://bit.ly/HiddenBrainChecklist
- Cockpit Checklists: Concepts, Design, and Use http://bit.ly/CockpitChecklistOWASP
- Human Factors of Flight-Deck Checklists: The Normal Checklist http://bit.ly/HumanFactorsChecklists
- A Surgical Safety Checklist to Reduce Morbidity and Mortality in a Global Population (NEJM) http://bit.ly/SurgicalSafetyStudy
- Safe Surgery (WHO) https://www.who.int/patientsafety/safesurgery/en/

Joe Kuemerle - @jkuemerle

https://github.com/jkuemerle/OWASP-DC-2019