Using Checklists to improve Information Security Operations

Leadership essay

Author: Balaji Balakrishnan <pingbalaji@gmail.com>

Advisor: Stephen Northcutt

Accepted: January 10th 2015

Abstract

The inspiration for this essay is from the incredible book "Gawande, A. (2010). The Checklist Manifesto: How to Get Things Right".

Checklists started way back in aviation industry. Aviation industry reduces casualties by following concise checklist for all activities. Pilots trust check lists and they continuously improve the check lists with expert feedback and testing. Construction industry is able to build sky scrapers and architectural marvels without any structural damages by following check lists. Finally the author explains how check lists were used in medical industry to improve patient safety during surgical procedures. There are three types of problems the author explains, simple, complicated and complex. Information security problems consist of all types.

In this paper we will review sample prototype checklists for few problems with some research references. As our industry leaders have been suggesting we cannot stop or prevent breaches against determined adversaries but we can make is difficult enough that they move to easy targets. If the pilots can use check lists and provide a highly reliable flying experience, If construction companies can build sky scrapers with high precision withstanding natural disasters, If doctors can use check lists to improve patient safety maybe it is time information security industry also followed simple and effective check lists to improve incident response and reduce impact to our organizations.

Follow pre-established checklist

The below tool to improve incident response is from the incredible book “Gawande, A. (2010). The Checklist Manifesto: How to Get Things Right”.

In order to prevent mistakes during incident response the best approach is to have check lists to follow during critical incidents and have them tested during regular intervals so everybody is clear what the next steps are and focus on engagement for better team work to remediate the incident. By not panicking and following a clear established checklist the incident response team engages cognitive thinking and enables the success of the team. Following checklists engages the deliberative system and provides efficient results.

Checklists started way back in aviation industry. Aviation industry reduces casualties by following concise checklist for all activities. Pilots trust check lists and they continuously improve the check lists with expert feedback and testing. Construction industry is able to build sky scrapers and architectural marvels without any structural damages by following check lists. Finally the author explains how check lists were used in medical industry to improve patient safety during surgical procedures. There are three types of problems the author explains, simple, complicated and complex. Information security problems consist of all types.

Simple problems are for which we know the solution, say maybe patching systems before connecting online. But still people make mistakes in simple problem, maybe they are tired or maybe they forget which could lead to major consequence if one system admins forgets a minor step of patching. It is a no brainer that check lists will help with solving simple problems.

Complicated problems are like launching rockets where there is lot of coordinated activities with various teams but it is the same process every time. Even here check lists play a vital role where every team performs their check list and updates the remaining teams.

Complex problems are like raising a child or critical surgery where there are a lot of variables and there might be many uncertainties and complexities and one situation is not the same as another. This is applicable to critical security incidents since not every security incident is the same and it will involve various technology components and various teams. For complex problems the recommendation is to have check lists that include simple steps for following and involving key stakeholders with communication pause points where the different subject matter experts get together and decide the best solution for the situation at hand.

Why Checklists?

Checklists enable us to follow a methodical approach and reduce errors. Checklists engage us and force us to use the deliberative system.

Individuals have two systems of thinking—the automatic system and the deliberative system. The automatic system influences nearly all our judgments and decisions.

Below excerpt is from the paper MIND, SOCIETY,AND BEHAVIOR - World Development Report 2015. (2014, December 2). Retrieved January 5, 2015, from http://www.worldbank.org/content/dam/Worldbank/Publications/WDR/WDR 2015/WDR-2015-Full-Report.pdf:

"People who engage in automatic thinking can make what they themselves believe to be large and systematic mistakes; that is, people can look back on the choices they made while engaging in automatic thinking and wish that they had decided otherwise. Automatic thinking causes us to simplify problems and see them through narrow frames. We fill in missing information based on our assumptions about the world and evaluate situations based on associations that automatically come to mind and belief systems that we take for granted." Appendix A explains in detail the two systems of thinking.

Automatic thinking is good in most of the cases but in some cases it is error-prone since it takes shortcuts and approximates when we have not experienced a situation like new critical incident.

Information security resources are smart but will still make mistakes which leads to severe consequences either they are tired or because they would miss some critical steps during incident response.

Most of the security incidents happen due to human error and if there is a good incident response program the impact can be reduced. It is very important to engage the deliberative system during critical incidents.

Following checklists will engage the deliberative system and provides efficient results.

There are numerous other examples were check lists can be used in information security domain.

Simple problem

Checklists have been used for changing behaviors to solve simple problem like reminding public to wash hands regularly to prevent infections. Similarly simple checklists can be developed to educate and increase awareness among users for not clicking on phishing e-mails.

Complex problem

Checklists have been used for complex problems like medical surgeries. Similarly checklists can be developed for managing critical security incidents like DDoS or compromise related to sophisticated/APT threats.

Below is a sample incident commander checklist.

Responsibility	Activity	Action Taken
Incident Manager/Commander	Send initial email containing • Schedule for initial conference call, including bridge telephone number and access code that will be used for all meetings • Details of incident • Composition of Incident Response Team	

Incident Manager/Commander	Identify and assemble key stakeholders and incident response team(IRT)	
Incident Manager/Commander	Categorize and scope incident	
Incident Manager/Commander	Enter incident ticket	
Incident Manager/Commander	Assign incident owner	
Incident Response Team	Identify containment steps	
Incident Response Team	Identify internal stakeholders and communication protocols	
Incident Response Team	Identify external stakeholders and communication protocols	
Incident Manager/Commander	Schedule follow-up calls at scheduled intervals	
Incident Manager/Commander	Contact external media or authorities as required with liaison from legal and external communication teams	
Incident Manager/Commander	Notify the organizations management (CEO , CFO etc) as required	
Incident Manager/Commander	Complete post-incident/breach report	

It is important that the checklists are modified by the teams who are going to use it since it needs to reflect the team's incident response procedures and should be incorporated part of the overall incident response process. Once the checklist is developed the incident response team should develop table top exercises to practice the checklist and fine-tune the checklist.

Complicated problem

Checklists have been developed for complicated problems. Technical checklists for forensics are great example in information security domain. SANS instructor Rob Lee mentions in his classes to not be emotional and follow data driven methodology for incident response and forensics.

Below references has good guidance for technical checklists

IRM (Incident Response Methodologies). (n.d.). Retrieved January 5, 2015, from https://cert.societegenerale.com/fr/publications.html
MR-1 : Worm Infection
MR-2 : Windows Intrusion
MR-3 : Unix Intrusion
MR-4 : DDoS
MR-5 : Malicious Network Behaviour
MR-6 : Website Defacement

MR-7 : Windows Malware Detection
MR-8 : Blackmail
MR-9 : Smartphone Malware
MR-10 : Social Engineering
MR-11 : Information Leakage
MR-12 : Insider Abuse
MR-13 : Phishing
MR-14 : Scam
MR-15 : Trademark Infringement

Information Security Cheat Sheets and Checklists. (n.d.). Retrieved January 5, 2015, from http://zeltser.com/cheat-sheets/

SCORE: Checklists & Step-by-Step Guides. (n.d.). Retrieved January 5, 2015, from https://www.sans.org/score/checklists/

Sample Incident Handling Forms. (n.d.). Retrieved January 5, 2015, from https://www.sans.org/score/incident-forms

Conclusion

As our industry leaders have been suggesting we cannot stop or prevent breaches against determined adversaries but we can make is difficult enough that they move to easy targets.

If the pilots can use check lists and provide a highly reliable flying experience, If construction companies can build sky scrapers with high precision withstanding natural disasters, If doctors can use check lists to improve patient safety maybe it is time information security industry also followed simple and effective check lists to improve incident response and reduce impact to our organizations.

References

Gawande, A. (2010). *The checklist manifesto: How to get things right*. New York: Metropolitan Books.

MIND, SOCIETY,AND BEHAVIOR - World Development Report 2015. (2014, December 2). Retrieved January 5, 2015, from http://www.worldbank.org/content/dam/Worldbank/Publications/WDR/WDR 2015/WDR-2015-Full-Report.pdf

Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.

Information Security Cheat Sheets and Checklists. (n.d.). Retrieved January 5, 2015, from http://zeltser.com/cheat-sheets/

SCORE: Checklists & Step-by-Step Guides. (n.d.). Retrieved January 5, 2015, from https://www.sans.org/score/checklists/

Sample Incident Handling Forms. (n.d.). Retrieved January 5, 2015, from https://www.sans.org/score/incident-forms

IRM (Incident Response Methodologies). (n.d.). Retrieved January 5, 2015, from https://cert.societegenerale.com/fr/publications.html

Appendix A – Additional information on automatic and deliberative systems in Human brain

The book “Thinking fast and slow” which provided incredible information on how the brain works and the limitations. Human brain works in two systems of thinking - System 1(Automatic system) and System 2(Deliberative system). System 1 is more automatic actions , unconscious , limbic and emotional. System 1 - Unconsciously competent , know more , learning better , scaffolding structures ,experiments. System 1 is the intuition and sometimes intuition might be misleading so it is important to have engagement during the incident response process so system 2 is engaged. Emotions always overtake cognitive parts of the brain when emotions are on overdrive. When there is a critical incident there is a impulse , flight or fight response which takes all the energy and does not allow our system 2 cognitive part to take over. System 2 is the cognitive part or functions of pre-frontal cortex cortex which is called executive part of the brain which is unique to humans. System 2 has limited capacity. System 2 at any point in time can only perform 6 to 7 activities including remembering things/activities. Human brain has limitations and understanding this helps us realize how the check lists were effective.