Getting to Root

AFCEA
25 March 2021

Robert M. Zalaskus
Submarine Forces, Atlantic Director C4I (N6)
“Consistency, Reliability, Repeatability”

“Perfection” – we expect our paycheck to be accurate

“Control of a predictable process”
What Every Organization needs

“PROTECT OUR INTELLECTUAL PROPERTY, CLASSIFIED INFORMATION”

“SAFEGUARD CUSTOMER CONFIDENCE/MISSION ASSURANCE”

“SUSTAINED OPERATIONS”
What it takes

1. Work force competence (Training)

2. Eliminate single points of process failure (backup)

3. ???
1. Work force competence (training)

2. Eliminate single points of process failure (backup)

3. Work force FOCUS—“the secret sauce”; “mental weight training”; —an intangible quality that separates the mediocre from the brilliant
When things go wrong

- Organizations require:
  - Integrity
  - Introspection
  - Positive actions to reduce the likelihood of recurrence
Fictional Example:

“We want shipyard wireless to improve productivity in hull!”

*What could possibly go wrong?*

- Work force loses portable electronic device hardware – compromise of stored data
- Wireless not configured per accreditation requirements -- NNPI spillage
- Shipyard Servers compromised via hackers access to wireless network and inadequate defensive operations
  - Malicious code uploaded into shipyard servers
    - Loss of confidence in technical drawing database
- NAVSEA shuts down operations
  - Shipyard schedules must re-baseline
  - Planned work goes to other yards
  - Want ads emerge
You ask:

“Why is organizational leadership asking for a cyber security critique?”

• Loss of information and breakdown of defenses are at the heart of the crisis
  • Cyber threat assessment and adversary motive to exploit vulnerabilities,
  • Principles of cybersecurity
  • Management of risk to business and national security,
  • Tools of DCO, CND, RMF, . . .
Critique (there is no perfect or correct format)

• **Executive Summary** (What Happened and consequence “as a result…”)

• **Site Conditions**

• **Description of the Incident** (who did what)

• **Sequence of Events** (timeline – facts and problems)

• **Problems Identified** (Why it was a problem)
  • Reason for the problem – the current symptoms
  • Root Cause – the real problem

• **Corrective Actions** (short-term, long-term – aka “permanent”)
Executive Summary

• The Reason For Outage (RFO)
  • Frequently the end of many reports to leadership
  • Often light on the “so what”

• Example: On 01 April 2021, after failing to recover a lost shipyard production wireless tablet, a shop 67 worker choose another tablet that had not been configured for handling wireless confidential NNPI data. As a result, the shipyard network was compromised both from the lost tablet and through wireless access that led to the introduction of malicious code to the technical database. This led to a NAVSEA-directed shipyard shutdown, lost production, and the need to re-baseline all projects.
The shipyard was in full project production. A production efficiency initiative deploying wireless tablets into project hulls was approved and deployed.

Shipyard technical database was compromised when a wireless tablet went missing and presumed stolen from the work site. Subsequently, the use of a replacement tablet that was not fully configured opened vulnerabilities exploited by unknown hackers that uploaded malicious code into shipyard servers causing loss of confidence in the technical data before being undetected by SOC defenders.
On 01 February 2021 Shipyard Officials with NAVSEA concurrence authorized the secure wireless initiative deploying 20 secured tablets with plans to expand to 50 tablets.

On 01 March Shipyard security log entry identifies a lost wireless tablet serial number ####-####. After a 2-shift search of the workspace and interviews of the responsible shop workers, the tablet is presumed stolen and reported to local police.

On 02 March, Shop 67 obtains a replacement tablet from shipyard IT staff. To support tight production schedules, IT provides a brand new tablet contrary to SHIPYARDINST ####.

On 15 March at 2100Z, shipyard SOC reports event unusual database activity including synchronization and commit transactions. Potentially modified drawings with duplicate ID numbers identified in the technical database cannot be verified accurate.

On 01 April, shipyard SOC identifies a change in technical database administrator account and possible C2 channel using ICMP packets. The traffic was undetected by proxy-based firewalls. Activity traced back to 01 April events. Escalated to a cyber incident. Forensics team deployed.
Problems Identified

• 1. Shipyard IT leadership failed to develop adequate safeguards to prevent the loss of classified hardware in a production environment and measures to deploy only fully configured hardware to trained workers. The result was potential compromise of classified information on the lost device and use of unprotected wireless devices further risking compromise of data and the network.

• 2. Slow identification compromise by SOC defenders
Root Causes
(some categories)

**Technical** – (causal) – often the (RFO) problem statement
(Frequently where organizations stop)

**Operational** – individual actions/inactions
- DUE TO – some identified weakness
- DUE TO – some cultural, environmental, leadership weakness.

**Procedure and Training** – Individual/Group level of knowledge”
- DUE TO – some weakness in the procedure, training
- DUE TO – inadequacies in audits, oversight, quality

**Contributing Factors** –
Personnel (do we have the right people – DUE TO?)
Management Programs (were people qualified – did proficiency and refresher training lapse DUE TO?)
Human Factors (poor judgment, decision error – DUE TO?)
Root Cause

• Technical Root Cause: (Causal)
  • A shop worker used poor judgment left a classified laptop in an unsupervised
    work space and failed to safeguard classified hardware
  • Feeling a sense of urgency, IT back shift staff failed to control the provisioning of
    configured laptops.

• Operational Root Cause:
  • Shop worker complacency to use of classified wireless devices with inadequate
    sensitivity to protecting classified information DUE TO inadequate management
    oversight, audits, and monitoring of training effectiveness. As a result the
    management team failed to see the work force decline in safeguards and proper
    handling of sensitive equipment.

• Procedural and Training Root Cause:
  • Shift supervisors complacency in managing the in-hull work force DUE TO an
    assumption that workers handling tablets were following guidelines.
  • A gross lack of understanding by a junior IT staff resulted in issuing an un-
    configured tablet DUE TO an inadequate IT training program for new personnel.
    IT leadership failed to identify the training deficiency DUE TO an inadequate
    qualification program and inadequate product distribution controls.
Now what?

**Short Term Corrective Actions -- ~30 days**

- Disciplinary action?
- Review across the department/organization
- Update instructions/policy
- Fix material weaknesses
- Improve monitoring

**Permanent Corrective Actions -- ~90 days+**

- Update programs
- Change work culture
- Change organization priority and focus
Return on investment

- ROI depends on how the organization reacts to the analysis
- NR does not fire everybody for a reactor scram at sea
- We do eliminate the cause of factors leading to error and separate gross negligence from error.

- Corrective actions used as the basis of funding and manning
- ...no surprise that new funding and manning are not a substitute for prioritizing the resources in hand.
Take-aways

- **No points for recurring issues**

- **If subsequent critiques identify familiar problems, either:**
  - **Root Cause analysis missed the true underlying issue** e.g. organizational culture of treating cybersecurity as administrative rather than existential to our business
  - **Corrective actions were not properly constructed or executed.**
Take-aways

- **The goal is not to become good at critiques!**
- In my experience work force **focus** is often at the heart of error – multiple errors end up as incidents.
  - Increased training raises awareness – like caffeine, but does not correct the problem
  - Understanding why the work force does not pay attention is often a combination of environmental factors AND the work force limited appreciation of the importance of their work.
  - **Failure to focus is not root cause** If you cannot answer “DUE TO” then we are just articulating the problem

- **Organizations have fewer incidents when workers know:**
  - Its a job worth doing
  - The organization recognizes and values personal contribution
  - The worker see what they do is an investment toward their personal goals and future
“Success at anything will always come down to this: focus and effort. And we control both.” Dwayne Johnson (The Rock)

“Who looks outside, dreams. Who looks inside, awakens.” Carl Gustav Jung (1950’ Swiss psychiatrist and psychoanalyst who said something that fit this discussion, but probably never had to do a root cause analysis.)
Questions