THE INTRICATE SECURITY CULTURE ISSUE: SOME CONSIDERATIONS ABOUT THE ROLE OF MANAGERS

C. SPEICHER
Ministry of the Environment, Climate Protection and the Energy Sector, Baden-Württemberg
Stuttgart, Germany
Email: carsten.speicher@um.bwl.de

Abstract

The paper deals with the importance of a positive leadership for a well-fostered nuclear security culture in practice and the impact that the behaviour of managers can have to it. The noble goal of a robust and positive security culture is not restricted to the classical security system but is also indispensable for an effective cyber security culture as well. While it is easy to state and demand for appropriate management skills of executivess, this question is quite intricate when it comes to the adequate leadership behaviour and its effects to the security culture of the overall staff.

INTRODUCTION

One problem may arise from the fact that the goals of the organization are – maybe - not 100% identical with the goals of its staff and another problem is the definition of a good leadership itself as it remains somehow vague or dizzy what good leadership is based on. At times people are promoted to a position where higher leadership skills are necessary than they can actually prove at this time. Taking this effect into account in a rather funny way, you could think about Peter Principle. The Peter Principle can be describes as the tendency in organizational hierarchies, such as that of a corporation, is for every employee to rise in the hierarchy through promotion until they reach their personal level of incompetence. Incompetence is the one of the worst threats for organizational culture. What does culture mean in this context? Culture – in general - means for a group of people what personality means for an individual. Culture is the sum of everything we learned and everything what is considered by the group to be a value (FIG. 1). If we want to know where to go we at first we have to define our actual position.

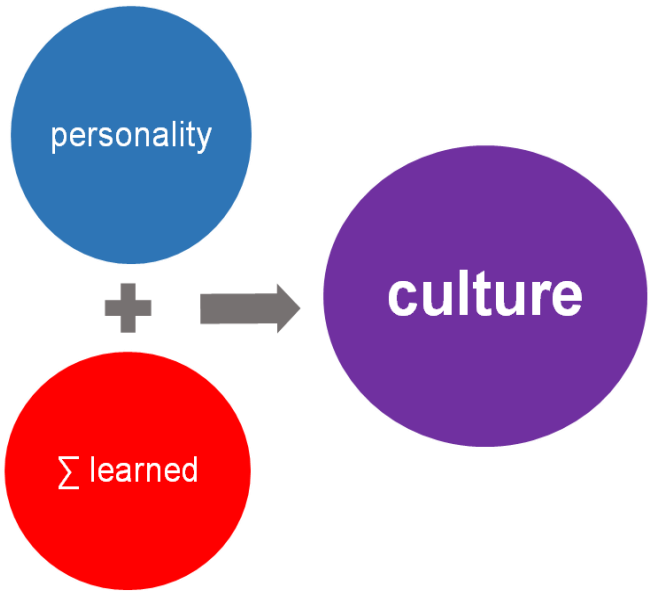

FIG. 1. Culture as the composition of different characteristics.

Is it therefore enough to keep the management systems in proper order? Although the management system itself may be posted as a high level goal of the organization, it highly depends on the degree of realization (the state of the art) and is furthermore cut down by the knowledge and discipline of the users (FIG. 2)

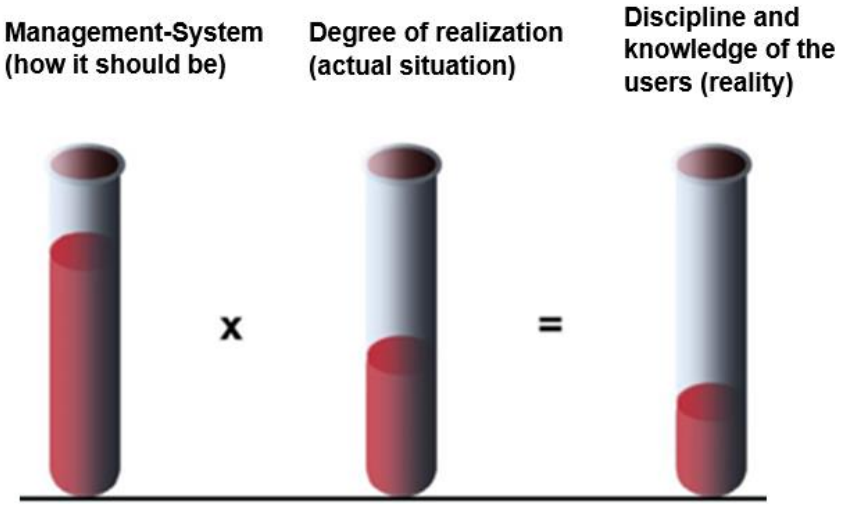

FIG. 2. The Effectiveness of the management system in reality.

It is somehow obvious that a perfect management system does not guarantee a perfect behaviour of the stuff. Moreover a permanent positive role modelling of the managers is indispensable to influence the staff's attitudes, espoused values and therefore their own behaviour. How can managers manage this?

1. EVERYTHING COULD GO WRONG

What could go wrong within an organization? Let's ask Mr. Edward Aloysius Murphy! In the real word: nearly everything can go wrong! As a perfect management system is still not enough we have to deal with malicious impacts of the human factor. To tell the truth there are also positive aspects of the human factor such as adherence to procedures, vigilance, a questioning attitude, professional work conduct etc. However in reality there remain some attitudes and thus negative kinds of behaviours that are highly connected to bad characteristics of the human factor. Some indicators may look like that:

- Unskilled and/or unaware guards
- "Lame"(weak) managers (Peter Principle?)
- Failing technology (too complex or not sophisticated enough, KISS principle or "complexity is the enemy of security")
- Unmotivated staff (mushroom-/crocodile-management by the managers?)
- Complacent managers (Dunning-Kruger-Effect?)
- Poor external working conditions („bad luck"…)

2. FOSTERING A ROBUST AND POSITIVE SECURITY CULTURE

Fostering a robust and positive security culture is not given by itself: it is based on a carefully chosen and balanced action by the managers who are in charge to act as leaders and role models for the general staff. Whereas the managers are supposed to guarantee a tailor-fit management system for themselves and their coworkers, the role modelling function of managers should not be underestimated. Taking into account the IAEA Nuclear Security Series No. 7 "Nuclear Security Culture" (implementing guide, 2008) one can easily identify the

characteristics of leadership behaviour which are dedicated to support a strong security culture of the overall staff, such as

(a) Expectations,
(b) Use of authority,
(c) Decision making,
(d) Management oversight,
(e) Involvement of staff,
(f) Effective communications,
(g) Improving performance and
(h) Motivation.

These characteristics should however be broken down and translated to a more handy or practical format. Besides they are expected to be more thought provoking than prescriptive because an effective leadership of the managers cannot be realized by simply parroting high but formal demands for the so-called appropriate behaviour of the managers. What does that mean in practice for the managers? They are indeed in charge of daily questioning their own attitudes and behaviour, e.g. by asking themselves some of the following questions:

- How do I guarantee to be regularly and often approachable for my staff?
- How do I take responsibility for the needs of my staff?
- How can I make sure to visibly act as role model when it comes to security related issues (and e.g. not claiming "special rights" and exceptions for myself)?
- What can I do to clearly and regularly communicate the security goals of our company to the staff?
- How do I contribute to improve the motivation of the staff?
- How do I make decisions in practice and do I properly explain them to the staff?
- How do I use authority and if so, every time if necessary and or just limited to sanction the staff?
- How can I clearly communicate the "red line" problem (the absolute "no-go" for our company when it comes to security related misbehaviour) and the obligatory consequences if crossing or violating this line?
- Do I regularly perform walkthroughs, make them visible for the staff and document them in a careful and respectful manner?
- How do I motivate and actively support the (self-)assessment of our own security culture?
- How do I contribute to implement the resulting action plan and monitor its progress?

2. THE DUTIES OF THE MANAGERS

Managers are therefore obliged and should feel responsibility to frequently reflect their own behaviour in regard to an overall strong security culture and optimize their own behaviour whenever necessary. Complacent or even ignorant managers should not expect a better security-oriented behaviour from their staff than from themselves. Only a positive and well-fostered security culture will contribute to an effective security regime and in addition most security related events are directly connected to a somehow negative human factor. Fostering the security culture is therefore an international obligation; terrorism and criminal acts do not stop at borders, but before trying to improve the current state one has to characterize and analyze it to be able to derive improvement measures. Performing a self-assessment of security culture seems to be a valuable tool to do so and may lead to self-reflection about the own role and self-responsibility (awareness!). A toolbox how to perform such a self-assessment is already offered by the IAEA NSS 28-T ("self-assessment of nuclear security culture"), it should however be tailored to the considered application. Some instruments to improve the current state of security culture are described in the IAEA NST027 ("Enhancement of nuclear security culture"). Whereas it is an international obligation to foster a robust security culture to turn the human factor into a positive drive, the licensees can profit from that even in regard to economic reasons (in reality only safe and secure operation means production). Like health insurance does not prevent you from falling sick, a campaign to support and enhance your security culture may reduce possible implications of events that cannot be completely avoided (mitigating effects). Therefore efforts to foster a robust security culture should be considered as an investment in the future. Self-assessment of security culture should be a voluntary organizational tool of the operator, therefore voluntary participation and anonymity should be guaranteed. The regulator may motivate and support the licensee to perform such a self-assessment; sanctioning (also by the regulator) in regard to possibly bad results may lead to (another…) data graveyard (happy talking of the operator's top management to calm the regulator); this would however do not help anybody.

It is the holy duty of managers to fight against incompetence at any level of hierarchy because on the one hand incompetence may lead to bad work performance and on the other hand it can increase the gap of knowledge by missing negative feedback (FIG. 3). Finally such a bad management of failures increases the incompetence without any corrective action to improve the overall organizational culture.

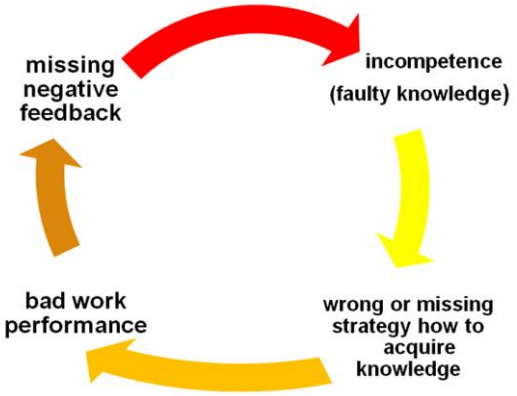

FIG. 3. The vicious circle of incompetence.

4. WHY AND HOW TO FIGHT COMPLACENCY

Complacency can be describes as a feeling of contented self-satisfaction, especially when unaware of upcoming trouble. This symptom can – unfortunately - be observed within any organization esp. at higher levels of hierarchies, as reaching this level may be considered as reward for previous performances. Weak leadership behavior may feed complacency down the leading line (FIG. 4) so that complacency can be found as a bad principle within all parts the organization which weakens the vigilance as well as the failure culture.

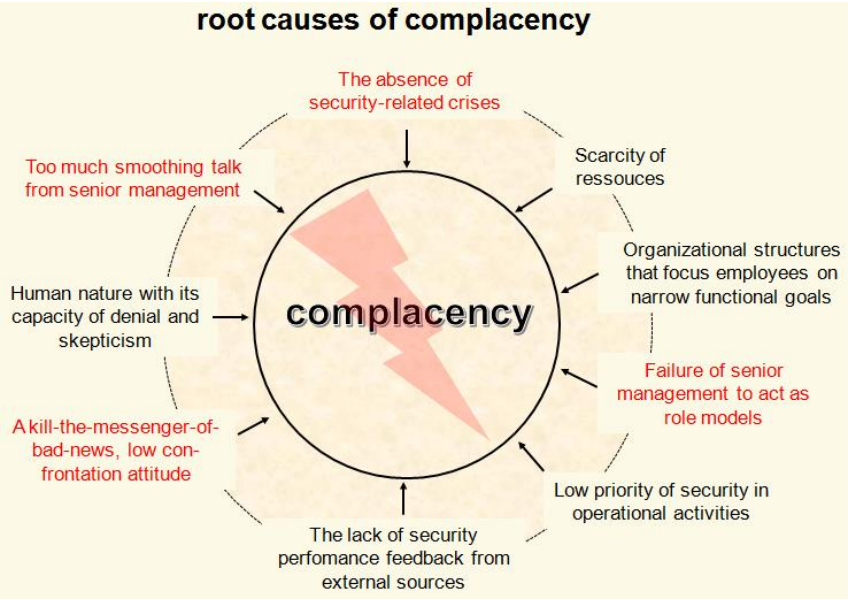

FIG 4. Various negative managerial factors may feed into complacency of the staff.

Complacent behavior may also weaken the will to report, analyze and fight minor errors or near misses. Remembering Helmreich's error pyramid an accumulation of observed but unreported work errors may finally lead to serious accidents (FIG 5.). It is therefore mandatory for managers to create and foster structures to carefully analyze such "low-level" errors and derive some corrective measures to prevent further damage for the organization and its environment.

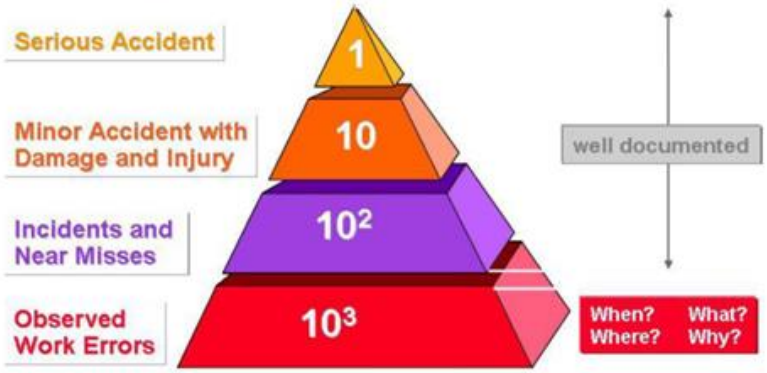

FIG. 5. Helmreich's error pyramid.

To summarize this intricate situation we should take a look at the reasons why minor errors are so rarely reported. A cornucopia comes into question here:
They are so rarely reported as

- they are not considered to be important,
- they are not identified as errors,
- staff is afraid of "extra" work,
- staff fears sanctions,
- staff is afraid of "loss of face" or
- staff is "simply" demotivated: "I have already reported something so many times. And nothing happened afterwards because people don't take it seriously".

A proper and profound error analysis is essential for any organization not to climb up the error pyramid. A kind of permanent staff position is highly recommended to cope with this task and procure the exchange of experiences within and from outside the organization. This staff position should (mostly) be in the position to work "outside" of a direct command line. Once again: regular self-assessments of the organizational culture may contribute to the insight of what goes wrong within the organization and what can be done to improve the level of awareness and feelings of self-responsibility for any member of the staff. The results of different pilot projects of self-assessment campaigns in Germany reveal that staff – in general – is interested in security related topics but on the other hand rather thinks that it is not well informed about security which can be deduced by some answers within self-assessment surveys such as

- the availability of information about security related topics should be increased,
- there should be special courses on security culture incl. a Q&A session where there is a place for open and frank discussions as well,
- managers should also communicate security related goals,
- when updating security related rules and guidelines, special attention should be paid to clarity and unambiguity,
- training and qualification should be improved,
- managers should improve their walk-throughs (personal note: either they are not performed or they are not realized as managerial and
- parts of the staff expect from their bosses a greater attention and appreciation of their work.

4. FINAL CONCLUSIONS

There is a myriad of references, literature and courses what managers can do – or better – should do to be good leaders and to improve the organizational culture within their companies. Alone the knowledge of what should be done is insufficient without deliberate actions. Before planning any action managers should bear in mind the following ideas and thoughts to enhance the organizational culture and improve their own behavior and attitudes (FIG. 6):

- Every human is fallible, that is our nature, therefore organizations should not only rely on hope that the "last barrier of defense", the fault-free operation, protects us from incidents.
- Security culture, as well as safety culture.....

..... is what is happening when the boss is not observing and
..... starts at the top level of an organization!

- Therefore managers are in charge to…
  …appreciate the values of your staff,
  …understand the values incorporated by the subcultures of your staff and
  …motivate necessary changes in good alignment of the already existing values.
- Security culture does not have to be (re)invented or created from scratch: it is already existing but can me optimized punctually at least!
- Each investment in security culture is an investment into the future that (unfortunately) cannot be quantified by € or $.
- Self-assessment of security culture is a management tool of any organization involved and not a data graveyard for the regulator.
- Self-assessment must be (tailor) fitted to the respective organization and its own culture; there is not any "one fits all tool"!
- The effort for a self-assessment should be reasonable, but the benefit could be significant (KISS principle vs. salesman's dreams)
- Self-assessment is neither the only source of information of the state of the security culture in practice nor does it replace any security measure.

FIG. 6. Nutrition for a positive organizational culture.

ACKNOWLEDGEMENTS

I would like to thank Dr. Igor Khripunov (CITS, University of Georgia/USA) for his extremely valuable expert advice and great encouragement throughout implementation of the self-assessment methodology as well as Mr. Axel Hagemann (the German "founding father" of tools and tricks to evaluate and promote the nuclear security culture) to introduce me to the intricate challenge of evaluating and quantifying the state of (nuclear) security culture.

REFERENCES

[1] J. KRUGER, D. DUNNING "Unskilled and Unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments", Journal of Personality and Social Psychology, Vol. 77, No. 6 (1999), 1121-1134.