How to Transfer Cyber Security Skill?

MILICA D. DEKIĆ, Subotica

Professional paper

UDC: 343.53:004.738.5

DOI: 10.5937/tehnika2203399D

Cyber defense is a challenge to be taught as it seeks from attendees to adopt real technical skills. Skill is a capacity to resolve some practical problem, but sometimes it’s needed to cover such a capability with theoretical background in order to better understand that area of interest. Teachers transferring such a skill must be well-educated and in position to create engaging course and training which can give an opportunity to attendees to take the most from such a lesson. In this article, we will stress out ongoing methods in producing cyber security workforce and highlight education as a strategic factor of any community, so far.

Key Words: cyber security, education, intelligence, criminology, technology

1. INTRODUCTION

In practice, skill is ability to tackle a set of theoretical and practical concerns while on some task. Role of education is to provide a smooth transfer of once explained knowledge, exercises and reasoning methodologies. Cyber defense is part of safety and security sciences and practices and it needs a very comprehensive approach in order to be learnt. As it is a defense area it can be used for both – business and service purposes. The most trickery thing with information security is it requires a multidisciplinary access as today’s technology is getting well-controlled and in an entire technical ecosystem there is a need to manage inner and outer threats to overall solution. In control engineering, threat could be assumed as a disturbance to some object or process, but the outer risks are mostly man-caused. Indeed, inner risks could be correlated with some human activities as well and they are usually seen as an insider threat action. In other words, modern technological systems are not only strictly linked to synergy of engineering disciplines, but they rather make touch with some social sciences in order to expose their multidisciplinary approach in any sense. Cyber defense is a field which exists several decades and in time of 4th industrial revolution it made its progress in everyday life. Very appealing stuff in this case is ongoing technical infrastructures are vulnerable on hacking attacks and such a weakness could be exploited in any kind of information warfare. Imperative of good defense is to protect its people and assets from being hurt in any empirically possible scenario.

Some expert’s streams suggest increasing awareness about current situation, but every new day brings with itself emerging criminal schemes and challenges. Good news is in both – civilian and law enforcement environments it is feasible to respond to such a concern, so majority of those cases are completely resolved in time consuming fashion. Apparently, any incident in cyberspace can be recognized as high-tech crime and in such a sense it’s clear why cyber defense is a science which guidelines should be carefully transferred though intelligently prepared education sessions. Some predictions say that future tendencies will demand minimal arrangement of human workforce in cyber security branch. That does not mean people will be excluded from IT industry, but inventions of tomorrow will dramatically reduce need for human role in assuring information-communication infrastructure putting point on current cyber skill shortage. It appears education of coming time will offer deeper expertise to many and we will literally live in the world of knowledge. On the other hand, skill we are familiar with today will become the matter of past, so cyber instructors will probably need to deal with a plenty of R&D findings in order to transfer their skill to future users of cyberspace. Explaining someone how to make something needs skill and total role of instructors could seek good understanding of next trends and tendencies. In our opinion,
Many education providers worldwide offer learning programs to their students. Those candidates are qualified for work and defense demands as they can get chance to serve in industry, as well as security sector. Security organizations on their own can provide some training to their member and those courses are well-planned and usually suitable for serving with some security tasks. Also, civilian programs in cyber defense also cope with prefix defense and if not on service those professionals are in touch with local authorities as they might give critical findings about some threats in cyberspace. Cyber defense training for business is more user experience oriented, while education in security is strictly specialized and addressed to great skill transfer. Cyber security education surrounding is huge marketplace and does not matter how coming technological development and progress will go there will always be place for skillful educators, trainers and instructors. Point with prospective tendencies in science and technology is we will live in much secure world, so present cyber physical systems will need more professional workforce to produce value in terms of products and services. In other words, we will be in position to improve productivity and undoubtedly enrich our economies relying on technology which will provide safe environment to work in. Next trends promise better security to everyone and in decade or two such a visionary effort might become reality as our civilization is taking that direction. Best investment into future is education and does not matter how far away humankind will go we will chronically need a skill for resolving problems and that is feasible only through well-developed knowledge transfer procedures and policies.

2. BACKGROUND INFORMATION

Cybercrime is a crime area according to international policing doctrine as it can cause harm to anyone being target of such a campaign. Purpose of high-tech security is to prevent, monitor and respond to any anomaly in cyberspace assuring safety and security to all members of communication-information ring. Science dealing with criminalities is criminology and it is purely social discipline. In other words, cyber defense is not the matter of technology only – it’s more like multi-field mix of engineering and criminology. Hence, that’s why it is needed to cope with multidisciplinary insight into cyber security as such an area is much more complex for studying as it might appear at first sight. On the other hand, criminology is practice which requires a deep understanding of laws particularly the Criminal Code as anything happening in cyberspace could be assumed as someone’s criminal responsibility. Apparently, education and training programs in combating cybercrime must provide comprehensive skill transition from instructor to attendee. It seems there will always be need for education as human beings must instruct and show to their offspring how to do or make something. Current tendencies indicate if we assure cyberspace and offer safe progress to everyone on the planet Earth we will mainly teach new generations how to make something putting entire conflicting and unsafe time into history. In our opinion, time of crisis is with us for a long period of time and only applied science can put us on track of development and prosperity. Modern emerging technologies and their infrastructure are designed to catch any possible activity relying on their networks. That means whatever is done in cyberspace will leave trace offering best practice in criminology to significantly reduce amount of crime in community. In total, with technological growth and development threats have become common part of technical sciences and as we had time to put all technological solutions under more or less similar standards ongoing appeal in science and technology could be to remove all potential risks coming from inside or outside, so far. Challenge is tackling and probably time consuming, but we believe real outcomes will be measurable in future.

3. MISUSING CYBERSPACE IS A CRIME

Cyber defense is a strategic matter today as emerging technologies become unavoidable part of our lives and businesses. Computer, internet and communication advancements get their mass application with days that come. Majority of industrial activities are happening in cyberspace and any flaw in such a sense can impact non-returnable losses to society and economy. Cybercrime costs global economy trillions of dollars per annum, so does not matter how hard someone works cyber criminals will take advantage over that effort and hug good portion of profit. In other words, someone will do everything to make something and someone else will enjoy benefits. That’s totally unfair and in such a manner typical sort of robbery. In addition, there is always a fear from some kind of information warfare which can be true threat to many people. Cyber security got its root in previous century, but even now that area is under focus. Literally that overwhelming with new technologies is making situation in high-tech space such an important. Therefore, if we talk about occurrences in cyberspace it’s obvious it’s needed to look for schooled and well-trained workforce which must have a skill to tackle any concern on the web. As suggested information-communication technologies are on fire nowadays and point is
to develop cutting-edge systems which can protect entire infrastructure automatically. Indeed, it’s needed to push up modern requirements in industry as any technological projects of today must be initialized with cyber defense updates. Information security is from vital significance at any R&D stage and in order to touch such a demanding level it’s needed to invest into education. To use options of cyberspace it’s needed to cope with skill. That includes both – offense and defense, so challenge to education is how to share that knowledge with staffing. Any intentional or unintentional anomaly in cyberspace brings with itself criminal responsibility and huge numbers of those cases have their epilog on court. Reason for that is many countries across the globe deal with more or less developed legal regulation in cyber security, so their Police Forces can investigate and prove those crimes seeking very severe punishments to such offenders. In other words, cybercrime and hacking are criminal justice responsibilities, but they need technical skill in order to be managed as a case with authorities. Skill is needed in any fashion either on side of bad or good guys and goal of security is to overlay threat.

4. BUSINESS APPROACH TO EDUCATION

Interest of any competitive legal business is to make a profit as it means it will operate with advantages leaving positive track record of its functioning. Hackers are those who can make drawbacks to such an organization and logically there is a strong need to overcome such obstacles. Civilian sector is extremely vulnerable to cybercrime as majority of those assets belong to critical infrastructure. Overall economy, society and people’s security could be challenged via any sort of high-tech attacks. Moreover, it’s about asymmetric situation where very few of them can shake wellbeing of many. Business landscape is especially sensitive to so as it makes money and once targeted by hacking groups can collapse in quite short period of time. Cybercrime is taking part anytime and anywhere as we yet need adequate response to such a crime area. Entire case management can take time as it is needed to collect evidence following strictly defined procedures. With strong business environment it’s possible to count on better standard, progress and prosperity to all, but IT crime is something that brings unrest to total civilian community. To our experience it’s about entire social maturity and people’s capacities to cope with rules, responsibilities and obligations. It’s not feasible to offer some trusted role to someone irresponsible as that staff can demonstrate carelessness and absolute absence of attention about business needs. Next, here we have education on scene! Some business employees could have educational background in computer science and information security, but rest will not cope with any such qualifications and they will need to be provided with well-developed training program which will give them chance to get along with some basic concepts. Cyberspace is literally overwhelmed with such annoying contents and no competitive business wants to be robbed or cope with any kind of discontinuity. Time is money! Main challenge with transferring cyber security skill within business surrounding is not many staffing will be motivated to accept those new habits. In other words, instructors must create engaging sessions trying to teach attendees as good as they can. Once attendee deserves confidence, easiness in resolving concerns and time effectiveness we can say skill transfer was successful. New times come with new tendencies and in such a reason it’s important to provide continuity with skill transfer as novel challenges can be far more different than previous ones.

5. DEFENSE OVERVIEW TO LEARNING

Majority of defense agencies look for training which can offer skill-based learning. It’s difficult to obtain skill, as well as to use it for smart applications. Point with such an approach is someone being trained to some task should show certain level of thinking outside of box as those outcomes could be applied in resolving practical issues. Defense organizations need staffing being capable to accept routine as such a field is highly demanding and requires good portion of concentration on task.

New ideas in such a case are more than welcome as they can provide authentic paths and some degree of effectiveness in resolving problems. In our understanding, mix of defense and technology is needed in order to cope with best practice in criminology and that routine approach is mainly correlated with solving technical problems. In other words, usage of technology can become someone’s habit, while tackling case seeks from officers to follow ingenious pattern. In practice, skill transfer for defense needs well-prepared instructors which can offer equally qualitative lecture notes and exercises to their attendees. Consequently, staffing must adopt great understanding of both – theory and practice as they could obtain their tasks.

Mission of security is to protect legal interests of any nation or country, so that’s why anything being in touch with so has critical connotation. For such a reason, it’s clear why educating defense members is from strategic significance to many. Skill transfer capacity is something that cyber security instructors must possess as their role in managing needs of defense community is very sensitive. Above all, knowledge transfer in defense is more like hierarchy-oriented and required training to such a community must be applied
only to candidates that are passing some scale of selection on their service.

6. POINT IS A BALANCE

Security is an area that needs balance between offense and defense in order to make risk being manageable. Similar situation is with its education as it seeks harmony, as well as very strong rules following. Role of cyber defense is to make order within cyberspace and coming tendencies suggest automatically governed systems can accomplish that better than human workforce. It’s important to mitigate risk from solutions being threatened as forces of offense and defense would be in perfect balance. New time brings new trends and in such a manner we must rely on computers as they can process information much faster than people. Indeed, machines should serve to human beings as they are created to provide convenience and problem-solving capacities to all of us.

7. DISCUSSIONS

It looks like paths we go are pretty tricking and maybe we expect they will lead us somewhere, but they might mostly direct us to end street. Time of crisis made us facing up so unsuitable lessons and it appears future will seek from us more responsibility and no right to mistake. History is a good teacher, but sometimes we are not capable to master all those warnings coming from so as we might cope with chronical lack of awareness and linkage about situation that is passing next to us.

7. CONCLUSION

Transferring skill is a big deal especially if it is needed to make that transit within cutting-edge zone. Only constant thing in the Universe is change and it depends just from us how well it will be handled by humankind, so far.

8. ACKNOWLEDGEMENTS

Milica is such a truly thankful to her family for all their love, care and support throughout her life, schooling and service.

REFERENCES


REZIME

KAKO PRENETI VEŠTINU IZ VISOKOTEHNOLOGIJSKE BEZBEDNOSTI?

Visokotehnološka bezbednost je izazov za podučavat i, jer zahteva od polaznika da ima pravu tehničku veštinu. Veština je kapacitet za rešavanje praktičnih problema, mada je ponekad potrebno posedovati i teoretsko znanje kako bi se oblast bolje razumela. Predavači koji prenose tu veštinu mogu da budu školovani i u stanju da uključe polaznike u svoju nastavu. U ovom članku ćemo obraditi tekuće metode u proizvodnji kadra za visokotehnološku bezbednost i naglasiti obrazovanje kao strateški factor zajednice.

Ključne reči: visokotehnološka bezbednost, obrazovanje, saznanje, kriminologija, tehnologija