Understanding the Impact of Cyber Security Risks on Safety

Christine Izuakor
Department of Computer Science, University of Colorado at Colorado Springs, 1420 Austin Bluffs Parkway, Colorado Springs, U.S.A

Keywords: Security, Cyber, Safety, Risk Management, Risk Assessment, Impact, Confidentiality, Integrity, Availability, Aviation.

Abstract: To date, cyber security risk management has focused on preservation of information security through protection of confidentiality, integrity, and availability (CIA). The growing use of cyber technology in safety intensive organizations has posed a challenge for those trying to understand the impacts cyber security risks have on safety. This knowledge gap slows progress towards InfoSec maturity and puts organizations and stakeholders at greater risk. For example, e-enabled aircraft now rely heavily on cyber resources, yet cyber security analysis in aviation usually focuses on CIA of information to prevent economic loss. What happens when a malicious attacker successfully exploits cyber aircraft vulnerabilities? This can potentially downgrade critical functions and result in injury or loss of life. To better understand the impacts of cyber risk on safety, the CIA information security triad should expand beyond its current focus to also consider safety.

1 INTRODUCTION

As technology continues to evolve and grow in use, risk management plays an integral role in ensuring that such technology does expose organizations to cyber-attacks. Successful cyber-attacks can negatively impact economic security and safety, and are currently an inherent reality that any sustainable organization or industry will face. For example, the transportation sector provides a great example of technological growth and evolution that can result in innate risks. 25 years ago, aircraft were not e-enabled, cab fare could not be paid using smart phones, and automobiles did not include internal computer systems with remote access. Today, all of these features exist to provide a more convenient and optimal experience for the user, yet expose the sector to new cyber threats.

A key step in the risk management process is understanding the impact, if such threats are to become active risks (National Institute of Standards and Technology, 2012). The impact of cyber threats, especially in business settings, is commonly measured in terms of economic loss. Examples include, but are not limited to, the value of information lost, brand damage, directly stolen funds, and reduced revenue from system outages. The consequence measurements are monetary; however, motives are not limited to monetary gain. Research firm TrendMicro, for example, cites information theft, espionage and sabotage as motivators for cyber-attacks (TrendMicro, 2015). These motivators can all result in safety impact.

Recent reports of a researchers attempt to hack an in-flight entertainment system on a commercial aircraft and access the avionics control system are an example where monetary loss is no longer the greatest concern (Zetter, 2015). Though the International Civil Aviation Organization discredits similar claims due to checks and balances of the aviation systems (International Civil Aviation Organization, 2014), if an attack were successfully executed the impact would likely exceed monetary loss and include safety.

Thus, an impact not adequately discussed and understood in the cyber security realm is the intentional or unintentional consequence of cyber risks on safety. This provokes questions such as: What impact can cyber security have on safety? Can a cyber-security breach potentially result in an injury or loss of life? The isolated perception that a breach in cyber security can simply be measured in terms of financial or informational loss needs to change. Additional research should also be completed to determine how security and safety coexist in this space. This will contribute to risk management in all industries, particularly those concerned with safety,

Izuakor, C.
Understanding the Impact of Cyber Security Risks on Safety.
DOI: 10.5220/0005796805090513
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 509-513
ISBN: 978-989-758-167-0

transportation, healthcare, and agriculture. Ultimately, the evolving nature of cyber technology calls for a new way of performing risk management; one that considers the impact of cyber risks on safety.

2 BACKGROUND

There has been some debate regarding the difference between security and safety. Merriam-Webster defines security as "the state of being protected or safe from harm." Similarly, safety is defined as "freedom from harm or danger" (Merriam-Webster, n.d.). In other languages, such as Norwegian, there is no difference between the two English words as the terms are used interchangeably (Albrechtsen, 2003). Researchers at a Norwegian university attempt to distinguish security from safety by associating one with deliberate harm and one with unintentional hazards, respectively (Albrechtsen, 2003). In my opinion, the difference is in the type of impact. Perceptively, safety focuses on prevention of injury, adverse health effects, and wellbeing of people. Security focuses on preventing the loss of tangible assets; whether information, buildings, functions, etc. One could argue that people are also tangible assets. While a valid argument, the loss of people from this perspective is usually in consideration of loss of function or value provided by people.

In the context of cyber technology, security is often described as the preservation of confidentiality, integrity, and availability of information. This fundamental triad defines the core needs of information and systems; Needs that, if impacted, compromise information security. Organizations concerned with safety, aim to prevent accidents and provide protection from physical, mental, or emotional injury. These organizations need an effective way to map these information needs toward safety.

3 ILLUSTRATION OF SAFETY IMPACT

Cyber security risks have raised safety concerns in several industries. For example, can e-enabled pacemakers leave patients vulnerable to cyber-attacks? Where e-enabled aircraft systems are segmented using firewalls, can these be bypassed by malicious intenders to execute unauthorized commands? Can nuclear weapons with remote trigger capabilities be activated? Each of these scenarios employs cyber technology for convenience, but also has the potential to gravely impact safety. There is work to be done when it comes to considering these trade-offs during risk management. Given the growing global concern of cyber risks to aircraft and the air traffic management system (International Civil Aviation Organization, 2014), the aviation sector will be used as an example of how cyber risks can impact safety.

The aviation sector is both security and safety intensive. The greater purpose of investing in civil aviation security is to protect people from any harm brought on, whether intentional or unintentional, by individuals with access to aviation systems. With good reason, airport security was heightened after the successful attacks of 9/11 to prevent an attack of that nature from reoccurring. More than a decade later, aircraft still remains an attractive target to malicious intenders seeking to "achieve surprise and maximize the destructive effect" (Department of Homeland Security, 2002) because these attacks result in loss of life, cause mass grief and terror, and decrease confidence in the aviation sector. As aircraft are becoming more comparable to a complex information systems, cyber-attacks in this sector can be targeted, not only for traditional financial or competitive gain, but to negatively impact safety and cause loss of life. Malicious attackers may see this as an innovative attack vector that airport security does not address. The reliance of critical aviation components on cyber technology creates exploitable vulnerabilities if not adequately managed.

Though theoretical demos, as well as real world events, have been documented involving cyber threats to aviation, (Storm, 2013), (Soperus, 2009), (Zetter, 2015), (Costin and Francillon, 2012) there have been conflicting views amongst aviation experts on the viability of successful cyber-attacks in aviation. The International Civil Aviation Organization released a working paper in 2014 reporting on risk assessment of cyber-attack against the air traffic management system (International Civil Aviation Organization, 2014). As an example, the report discloses that threats such as the disruption of aircraft separation data feeds could marginally increase the risk of aircraft collision. The report also states, "The ATC system has many internal checks and balances that make it very unlikely that a hacker can seriously compromise controlled traffic in controlled airspace. Most of the claims…have been made in ignorance of these system checks" (International Civil Aviation Organization, 2014). In order to make a risk management decision, in this case what appears to be "accepting the risk," there

should be a scientifically proven way to measure the impact of these risks on safety. Solving this challenge is imperative to the advancement of aviation security in this technological age.

4 CURRENT STATE OF CYBER SECURITY AND SAFETY RISK MANAGEMENT

In risk management, once a credible risk is identified, it can either be mitigated or accepted. In most cases, this decision is made based on the likelihood and impact of threat activation, consideration of existing mitigating controls and the cost to mitigate. Impact measurement is a key differentiator between cyber security and safety risk management methodology, and as such is the focus of this section.

Information security risk assessment frameworks published by expert industry organizations such as National Institute of Standards and Technology, provide enough flexibility in process for safety to be considered. The framework (National Institute of Standards and Technology, 2012) is used by risk management professionals in various fields and targets assessment of information technology. The approach begins with the identification of undesired consequences and impacts based on mission or business impact analysis. Critical assets associated with those consequences are then identified followed by threat identification. According to the framework, "assessing impact can involve identifying assets or potential targets of threat sources, including information resources (e.g., information, data repositories, information systems, applications, information technologies, communications links), people, and physical resources (e.g., buildings, power supplies), which could be affected by threat events" (National Institute of Standards and Technology, 2012). This allows a broad assessment of impact of cyber threats and supports the aim to understand how the loss of CIA impacts the organization on various levels.

On the other hand, safety risk assessment framework published by expert industry organizations such as Occupational Health & Safety Association (U.S. Department of Labor, 1992) and Canadian Centre for Occupational Health and Safety (Canadian Centre for Occupational Health and Safety, 2015) do a fair job of determining safety impact resulting from hazards. For example, the Canadian centre assessment begins with identification of hazards and then suggests measuring likelihood of injury or illness occurring and its severity to prioritize hazards. The ability to consider the impact of cyber risk lies in the ability to identify such hazards, but is not explicitly suggested. For an assessor that is not consciously seeking to consider cyber threats, this aspect of the assessment can easily be overlooked. There should be an awareness to deliberately consider cyber threats during safety assessments.

5 GAP DISCUSSION

Using risk assessment methodology in a typical organization, one may consider risk impact in terms of loss of revenue, damage to physical assets, and length of disruption. This information can then be used to determine if the risk should be accepted or mitigated. Though this is just one of many examples, using these impact categories alone can omit consideration of safety. It is possible that the same cyber risk can fall short of monetary impact thresholds, but could still result in injury or loss of life.

Therefore, it appears the gap lies in segregation of these two methodologies. Essentially, safety assessment does not consider all appropriate threats and cyber security assessment does not consider all appropriate impacts. Information security risk assessment methodology can facilitate evaluation of safety impact if applied appropriately, but often is not a concern of industries who use such frameworks. Similarly, safety risk assessment frameworks are effective for health impact analysis, but often focus on physical or traditional threats. The opportunity to incorporate cyber risks into these assessment is not currently being maximized.

6 RECOMMENDATIONS

Cyber risk assessment and safety assessment can no longer operate in silos. There is a need to understand how growing reliance on cyber technology in safety intensive organization impacts the bottom line: safety. There are existing initiatives that can be expanded and leveraged to address these concerns. For example, the SESAMO security and safety modelling project aims to integrate security and safety assessment together for development of embedded systems (City University London, 2015). This is a great effort, but focus is limited to a solution for embedded computing. The results of the project

can contribute to future research.

Additionally, the MITRE Corporation published guidance on evaluating the impact of cyber-attacks on missions (Musman, et al., 2010). Using a similar process, the focus on "missions" can be integrated with emphasis on "safety." Specifically, a model can be created that establishes safety related capabilities. For each capability, the normal expected operating level can be compared against the operating level after system impact has been realized. The resulting variance is a way to potentially view the impact of cyber-attacks on safety.

Other studies should be considered as well. Nevertheless, using the CIA model as a base along with cyber-attack characteristics outlined in the MITRE guidelines (Musman, et al., 2010), we can consider risks in the context of safety by simply starting with the high level model shown in Figure 1.

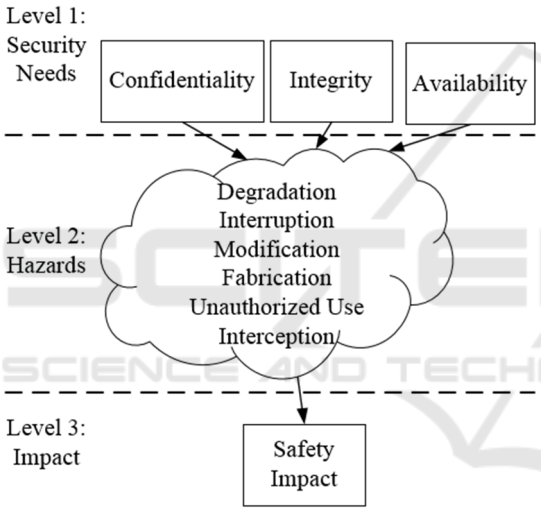

Figure 1: CIA Safety Impact Model.

Using this model, the following questions can be considered as a starting point for the assessment:

Level 1: Which component(s) of the CIA model is impacted by system failure?

Level 2: What hazards types can result from such failure?

Level 3: What impact do these hazards have on the organizational safety mission?

Additional research should be conducted to determine what scientifically proven mathematical algorithms may support the assessment and risk mitigation process inclusive of cyber and safety considerations. This should be engrained in general risk assessment, especially for those with primary safety concerns. Newer companies coming of age during the cyber era have the advantage of starting from scratch with technology and establishing risk management processes that adequately address cyber threats. Senior entities that were established well before these risks became of such great concern, have greater challenges and more work to do to achieve a reasonable security posture. The research and resulting methodology should be applicable to both of the aforementioned organization types. Working toward a new way of thinking when it comes to safety and security could be useful in all industries.

7 CONCLUSIONS

The growing use of cyber technology in industries with high safety risks at stake increase the need to understand the impact these attributes can have on safety. Existing information security risk assessment and safety risk assessment frameworks operate in silos and do not provide a cohesive understanding of how cyber risk impacts safety. By incorporating clear safety impact measurements into proven cyber risk assessment methods, there is an opportunity to gain a better understanding of how losses to information confidentiality, integrity, and availability can further compromise safety. Additional research is suggested to establish an algorithm for evaluating safety impact. In doing so, the algorithm or methodology could contribute to increasing security in transportation, health, technology, and other industries.

REFERENCES

Albrechtsen, E., 2003. *Security vs Safety,* s.l.: Norwegian University of Science and Technology.

Canadian Centre for Occupational Health and Safety, 2015. *Risk Assessment.* [Online] Available at: http://www.ccohs.ca/oshanswers/hsprograms/risk_assessment.html.

City University London, 2015. *SESAMO - Security and Safety Modelling.* [Online] Available at: https://www.city.ac.uk/centre-for-software-reliability/research/research-projects/sesamo-project.

Costin, A. & Francillon, A., 2012. *Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices,* Sophia-Anipolis: Black Hat.

Department of Homeland Security, 2002. *National Strategy for Homeland Security,* s.l.: s.n.

International Civil Aviation Organization, 2014. *Initial Report on Risk Assessement of Cyber-Attack - Air Traffic Management,* Montreal: s.n.

Merriam-Webster, n.d. *Security; Safety.* [Online] Available at: http://www.merriam-webster.com/dictionary/security.

Musman, S. et al., 2010. *Evaluating the Impact of Cyber Attacks on Missions,* McLean, VA: The MITRE Corportation.

National Institute of Standards and Technology, 2012. *Guide for Conducting Risk Assessments,* Gathersburg: NIST.

Soperus, M., 2009. *Conficker Work Shuts Down French and UK Air Forces.* [Online] Available at: http://www.maximumpc.com/conficker-worm-shuts-down-french-and-uk-air-forces/ [Accessed 20 September 2015].

Storm, D., 2013. *Hacker uses an Android to remotely attack and hijack an airplane.* [Online] Available at: http://www.computerworld.com/article/2475081/cybercrime-hacking/hacker-uses-an-android-to-remotely-attack-and-hijack-an-airplane.html [Accessed 20 September 2015].

TrendMicro, 2015. *Understanding Targeted Attacks: Goals and Motives.* [Online] Available at: http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-goals-and-motives.

U.S. Department of Labor, 1992. *VI. Risk Assessment.* [Online] Available at: https://www.osha.gov/

Zetter, K., 2015. *Feds Say That Banned Researcher Commandeered A Plane.* [Online] Available at: http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/

Zetter, K., 2015. *Is it possible for passengers to hack commercial aircraft?.* [Online] Available at: http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/ [Accessed 20 September 2015].