International Journal of Cybersecurity Intelligence & Cybercrime

Volume 1 | Issue 1 Article 7

8-2018

An Argument for Interdisciplinary Programs in Cybersecurity

D. Giever. (2018). *International Journal of Cybersecurity Intelligence and Cybercrime, 1* (1), 69-73.

COMMENTARY: An Argument for Interdisciplinary Programs in Cybersecurity

Dennis Giever*, New Mexico State University, U.S.A

Abstract:
In this commentary Dr. Giever presents a compelling argument for interdisciplinary programs in cybersecurity at the university level. He argues that we no longer have the luxury of allowing barriers to exist between those tasked with IT security and those who provide physical security. He recommends that any security program take an "all possible paths" or "balanced approach" to the protection of assets within an organization. Students in computer science, criminal justice, business, human resources, and others should work collaboratively within education programs learning these necessary skills. A team effort is needed to accomplish the myriad of tasks necessary to protect assets today. Graduates from such programs will possess the skills and abilities to work collaboratively on a comprehensive security design for their organization.

Cybersecurity has never been the exclusive realm of IT professionals. The protection of any asset, whether it is sensitive data, a laptop, or valuable merchandise in a warehouse, requires a comprehensive approach to asset protection. A security designer is required to address all possible vulnerabilities to the assets they are protecting. For a security engineer this simply means that we must have "balanced" protection (Garcia, 2008, p. 64). There is no shortage of examples of the convergence of physical and IT security. For example, in 2011 Cisco produced a white paper entitled, "Why Integrate Physical and Logical Security?" One of the first points made in this white paper is "As long as organizations treat their physical and cyber domains as separate, there is little hope of securing either one" (Carney, 2011, p. 2). Carney acknowledges some rather key points that add value to the arguments made in this commentary. For example, he points out that often the departments that manage the two types of security are entirely separate and often do not even collaborate (2011, p. 2). Kevin Ingram (2018, p. 3) adds to this point: "The bottom line is that it's easy, from a risk management perspective, to get distracted by the complexity of digital network security – firewalls and such – when some of the most gaping security holes can be in your physical premises." These statements clearly point to the need for a close working relationship between those tasked with both physical and cyber security.

*Corresponding author

Dennis Giever, the Academic Department Head of the Criminal Justice Department at New Mexico State University (NMSU) in Las Cruces, NM.

A fascinating example which might be of interest to the readers was outlined in the Special Report by the Office of Inspector General in June of 2017. The special report was the culmination of an event that had occurred at the 2016 Department of Energy Cyber Conference. At this conference a vendor, who was also making a presentation, placed a number of data collection devices in the common areas of the convention hotel. These "collection devices" were disguised as mobile device charging stations, but in reality were intended to collect specific information from any device connected to them (how often do you attach your cell phone or mobile device to a charging station at an airport or cyber café?). This incident was found to be innocent in nature as the vendor was using it as an example in a presentation, and the Inspector General's Office found that the "charging devices" were not designed to collect sensitive date – the point is obvious. A very clear and present physical danger presented itself (Office of Inspector General, 2017).

As part of this commentary, let me introduce the readers to a number of important concepts about a well-designed security system that demonstrate the need to address both physical and cyber security approaches to a balanced security system. It is useful to take a systems approach to developing a comprehensive security plan – whether you are protecting a physical location or a cyber-system. The Department of Energy has developed a very detailed process for the protection of physical assets which can, with only minor adjustments, be applied to cyber-systems. This process was initially developed for the protection of our nuclear assets, but was expanded in the early 1990s to any physical protection system. A number of universities around the country began introducing students to this systems approach to the protection of physical facilities. In the 2000s this process was also applied to cyber-systems. In the 2008 second edition of her book, Garcia specifically addressed the protection of cyber-systems (Garcia, 2008, pp. 307-314). To illustrate these issues in a little more detail, let me provide a short lesson in what the Department of Energy calls their DEPO model. For anyone who is interested in a more comprehensive review of this process, I would highly recommend a careful review of Garcia's 2008 book. To begin, DEPO stands for the Design and Evaluation Process Outline. As one might imagine, this is a rather complex and detailed process, but one that makes sense and can be applied to the protection of any asset.

The first step in the DEPO process is to determine the security system objectives. What are you protecting and from whom? This seems like a basic step, but it is critical and often overlooked. The next step is the design phase. What is critical at this stage is the concepts of "Detection, Delay, and Response." These three concepts are individually important, and it is critical that they be followed in the order presented. Delaying someone who is attacking your network is of little value if you do not realize that you are under attack. Your adversary can spend whatever time necessary to defeat your system – no one knows they are trying to access your system, so nothing is being done to stop them. The key is to detect a nefarious individual or individuals who are trying to access your system and then delay them. Once you know someone is trying to break into your system, you can establish protocols to delay their successful completion of the attack. Delay can take many forms, but it is critical to understand that its true purpose is to slow the attack while a response can be undertaken. The role of the response is to stop the adversary before they complete their task. In the physical world, that might be armed law enforcement arriving on the scene before the adversary is able to steal your stuff. In the cyber world, it might be nothing more than eliminating network connectivity, or sequestering the adversary or target system (Garcia, 2008, p. 312). One final critical component of the DEPO model is the analysis of the design. The key at this point is to test the effectiveness of your security system. Will it operate as designed? Will it stop your adversary? Careful planning along all stages of the process will help eliminate problems down the road. Proactively testing and evaluating your system is critical, rather than reacting following a successful breech.

While the design and evaluation processes are critical, there are a number of other important considerations. The Department of Energy presents three characteristics of an effective physical protection system: protection-in-depth, minimum consequence of component failure, and balanced protection. Once again, these same principles can be applied to cyber-systems or, for that matter, the protection of any asset. Protection-in-depth simply means that for an adversary to defeat the security system they must be required to avoid or defeat a number of protective devices in sequence (Garcia, 2008, p. 63). In principle, a good system will require differing skills and tactics for an adversary to successfully attack your facility. A single locked door is not enough, nor is a single firewall.

The second characteristic of an effective physical protection system is minimum consequence of component failure. As a security system designer, you want to ensure that your security system will not be vulnerable if a single component fails. Backup systems and a robust design will ensure that if a component fails, it will not render your entire system vulnerable. Of the three characteristics, balanced protection is the most applicable to this commentary. By definition, balanced protection means "that no matter how an adversary attempts to accomplish the goal (accessing your data, or stealing your stuff), effective elements of the physical protection system will be encountered" (Garcia, 2008, p. 64). For a physical system, that means whether they attack from the front door, back entrance, or through the wall – they will be detected and delayed while a response can be mounted to neutralize the attack. From our standpoint here, balanced protection means that, as a system designer, we must consider all possible paths to our assets. Whether a person is able to access your sensitive data remotely or whether they are physically able to steal a blade server – you have lost. The goal is to provide detection, delay, and response along all possible paths to your sensitive data.

The "all possible paths" approach to the protection of assets is the best argument for an interdisciplinary approach to security education. As Joem Wettern pointed out, "with all the layers upon layers of software-based security, we tend to forget about the vital role of physical security. The fact is, if someone gets physical access to your computer, they can pretty much do whatever they want" (2005, p.67). While it has become clear that the important role of both physical and cyber security is a well-designed security system, there is much more to security than just these two possible paths to your assets. What role does social engineering play in overall security? What about the insider threat? The hiring process is important, but equally important is the continued monitoring of all employees that have access to sensitive data. Security has evolved into a rather complex enterprise which encompasses a wide range of fields. The big question is what skill set does the security professional need today? And more important to this essay is what role does education have in providing this skill set?

Let me be so bold to say that I no longer believe that the necessary skill set can be possessed by one individual. A team effort is needed to accomplish the myriad of tasks necessary to protect assets today. The key, and the important role that education can play, is getting those individuals involved in working together to design an organization's security plan. Once again, this sounds straightforward and is much easier said than done. I have conducted security assessments (vulnerability assessments) at a number of organizations (both government and private sector), and a common theme is the lack of collaboration between these essential components. For example, in one international organization, the Director of Global Security was an ex-federal law enforcement officer. The physical side of security was well thought out and had the resources to develop a well-designed and well-tested physical security system. The problem was the folks on the IT side were understaffed and complaining about the lack of resources and, more importantly, the lack of respect they experienced within the organization. I have seen this from the other side where a well-funded and well-planned IT security infrastructure was in place, but the physical security folks were relegated to what amounted to night watchmen roles.

The folks on the physical side were underfunded and supervised by the same division responsible for grounds keeping and janitorial services. To complicate this issue even more, what roles do other divisions in an organization play? What role does human resources or the training division play in an overall security plan?

Let me circle back to two points made above. The first is social engineering. Often the greatest vulnerability to an organization is its susceptibility to social engineering. While a detailed explanation of social engineering is beyond the scope of this commentary, I would encourage readers to read both of Kevin Mitnick's books on the subject, "The Art of Deception: Controlling the Human Element of Security" (2002) and "The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers" (2005). Both of these titles will offer insights into how social engineers "trick" organizations into exploiting their security.

The second is the insider threat. As John Carney points out, "most security attacks occur from the inside" (2011, p. 5). Once again, while addressing the problem behind the insider threat is beyond the scope of this commentary it is, once again, critical that security personnel understand this vulnerability. I will point readers interested in this important topic to two rather dated books, but books that provide some fascinating insights into dealing with this issue. In the 1990s Gavin De Becker wrote two books that encourage individuals to utilize their instincts in dealing with threats of attack or violence. These two books offer readers a good understanding of what De Becker calls Pre-Incident Indicators. He also offers insights into how best to screen, manage, and if necessary fire employees. The books are "The Gift of Fear: and other Survival Signals that Protect us from Violence" (1997) and "Protecting the Gift: Keeping Children and Teenagers Safe (and Parents Sane)" (1999).

The major point I am hoping to convey to the reader is the need for all such divisions within an organization to be working closely together in the development of the overall security system. For this to truly work, each division must understand the role of the other divisions and, more importantly, respect the role that they play. This is where education comes into play. Well-designed interdisciplinary programs at the university level that bring together students from computer science, criminal justice, business, human resources, industrial and labor relations, accounting, marketing, and others is essential. Having students in all such programs working collaboratively together while receiving their education will provide the foundation for such working relationships when they join the workforce. The ability to break down the barriers or "silos" that often exist is critical. Cyber security personnel need to work closely with the physical security folks to ensure that all possible paths (access points) to the organization's sensitive information are protected equally (balanced protection). The folks in HR need to understand the important role they play in ensuring that all employees are properly vetted both at hiring, and throughout their tenure within the organization. Often, organizations are most vulnerable when they are terminating an employee. Cyber, physical, and HR personnel need to be working closely together when terminating an employee who might try to damage an organization's computer system. Planners and policy makers need to work closely with all such divisions to ensure that they too are part of the solution and not part of the problem. Everyone in an organization is critical to the success of a well-designed security system.

So what would a well-designed cyber/physical security program look like? For that matter, what would a well-designed comprehensive security program look like at the university level? The obvious answer is that it should be an interdisciplinary program that takes an "all possible paths" or balanced approach to the protection of all assets. Imagine students from computer science taking security classes with students from criminal justice, marketing, business, and others. Imagine a program that tasks students to develop strategies to protect assets from any number of possible attacks, for example,

someone trying to access sensitive data remotely. Another adversary may attempt to access that same data by physically breaking into a facility. What about the insider threat? How do we protect our assets from a disgruntled employee who has access privilege to our sensitive data as part of his/her job responsibilities? Imagine an educational program that provides a systems approach to security with an emphasis on balanced protection. Students from all of these disciplines will work collaboratively on a comprehensive security design. Students who successfully complete such a program would gain knowledge and appreciation for the important role that others within an organization might play in increasing the security posture of an organization. Most importantly, such students would develop the interdisciplinary skills to work collaboratively with divisions that might have seemed foreign to them. For example, having students in computer science gaining an appreciation for the importance of vetting all hires would be essential to understanding and, more importantly, dealing with a possible insider threat. Having an appreciation for rule of evidence and chain of custody from the criminal justice field might become critical if an organization chooses to prosecute a hacker. Understanding both physical and cyber threats should seem obvious. The true security designer of the future needs both the knowledge of, and more importantly, an appreciation of all of these aspects. They must truly understand this balanced approach to the protection of their assets.

References

Carney, J. (2011). White paper: Why integrate physical and logical security? CISCO. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/pl-security.pdf

De Becker, G. (1997). *The gift of fear: And other survival signals that protect us from violence*. New York, NY: Dell.

De Becker, G. (1999). *Protecting the gift: Keeping children and teenagers safe (and parents sane).* New York, NY: Random House.

Garcia, M. L. (2008). *The design and evaluation of physical protection systems.* (2nd ed.). Burlington, MA: Butterworth-Heinemann.

Ingram, K. (2017, February 9). Cyber risks threaten physical security, industrial controls. *CFO Newsletters.* Retrieved from http://ww2.cfo.com/risk-management/2017/02/cyber-risks-industrial-controls/

Mitnick, K. D. & Simon, W. L. (2002). *The art of deception: Controlling the human element of security.* Indianapolis, IN: Wiley.

Mitnick, K. D. & Simon, W. L. (2005). *The art of intrusion: The real stories behind the exploits of hackers, intruders & deceivers.* Indianapolis, IN: Wiley.

Office of Inspector General (June 2017). *Special report: The office of enterprise assessments testing incident at the 2016 Department of Energy Cyber Conference*. U.S. Department of Energy (OIG-SR-17-05).

Wetten, J. (2005, November). Time to get physical. *Redmond Magazine*, 67-68.