Advisory from Professionals

White Hats Chasing Black Hats: Careers in IT and the Skills Required To Get There

Eric Fulton
SubSector Solutions
345 Orchard Ridge Road
Kalispell, MT 59901
Eric@subsectorsolutions.com

Cameron Lawrence, Ph.D.
University of Montana
School of Business Administration
32 Campus Drive
Missoula, MT 59812
Cameron.Lawrence@business.umt.edu

Shawn Clouse, Ph.D.
University of Montana
School of Business Administration
32 Campus Drive
Missoula, MT 59812
Shawn.Clouse@business.umt.edu

ABSTRACT

The aim of this paper is to illuminate the exciting world in which "white hat crackers" operate and to suggest topics that can help prepare students to enter this high-demand field. While currently there is extraordinary demand for graduates to fill these positions that have relatively high starting salaries, employers find it difficult to hire students right out of universities who possess the right technical and social skill sets. The education needed to execute the requisite tasks is dynamic, broad and difficult, and there is a severe lack of qualified entrants into the industry. Accordingly, we suggest twelve subject areas to which students interested in the field should be exposed. The suggested framework is the by-product of the authors' industry experience, which includes presentations at Defcon and Blackhat. It is our hope that by describing the activities of "white hat crackers" and highlighting the basic social and technical skill sets required to be successful in this area, faculty members can become valuable partners in filling the pipeline with well-prepared graduates. We conclude the paper by suggesting that students in all business disciplines should have exposure to these topics that we consider to be an integral part of general information systems literacy.

Keywords: Information assurance and security, Certifications, Computer literacy, Computer security, Computer majors, Course development models, Ethics, General education, Security

1. INTRODUCTION: RED TEAM AT WORK

It's 7:45 a.m. on a brisk fall morning and I am staring at the midwestern headquarters for a major insurance agency from the edge of a nearby parking lot. The grey rental car I picked up the previous day is starting to get chilly, though I barely notice as I watch employees file into the building. Most of them enter through the main entrance, trodding past a

watchful pair of security guards and a badge-activated turnstile, finally disappearing into an elevator. I don't care about these employees right now. My attention is focused on the side entrance where I watch a steady stream of morning smokers pop in and out of a "secure" door to satisfy their nicotine craving.

Exiting my car I grab my briefcase, a pack of cigarettes and a cheap Bic lighter. I don't smoke, but that's not important. The fake RFID badge (the kind you touch to the door to authenticate) made in a hotel room the night before bounces against my leg as I walk up to the latest pack of smokers. I tap a cigarette out of the package as I strike up conversation. Sports is an easy and accessible topic to talk about and I'm quickly involved in the group. Fifteen minutes later I enter the building still embroiled in conversation until breaking off for a restroom, promising to continue the argument on the next smoking break. In the bathroom I calm my breathing down, grab a random piece of paper out of my bag, and begin my walk through the building. My main goal is to identify an empty cubicle and install a Pwnie Express Pwn Plug Elite, an excellent in-line computer that allows me to perform advanced technical exploitation from anywhere in the world. I begin walking around. The paper in my hand helps prevent me from getting hassled by other employees; people usually don't like bothering people who are focused, even if the focus is on a random paper in their hand.

Walking at a medium pace through the cubicle farm with one eye on my paper and the other scouting open cubes, I come to a stop at a row of empty cubes along the edge of the building. Each cube is equipped with a desktop just waiting for some poor new hire who will get stuck in this cubicle Siberia. Ducking into a cube I pull out my Pwn Plug and deftly connect it in seconds, finishing by moving some boxes to obscure its presence. It's doubtful that even if someone looked directly at the Pwn Plug they would know what its purpose is, but there's no reason to bring unwanted attention. As I stand, I hear an alert emanate from my pocket. Looking at my iPhone I see an SMS message telling me the Pwn Plug is active and on the network. Smiling to myself, I continue on.

The next stop is the copy station. Some companies have huge locked trash cans with slits cut in the top for paper; these dumpsters are used to "securely" recycle paper and prevent people from rummaging through discarded papers. This company, however, only has a box next to the copier that says "Recycled." Having seen no one for the past few minutes and now feeling rather bold, I stoop to grab the papers in the bin and neatly place them into my bag. As I ready to leave the office, a person approaches as I idle beside the copier and asks, "Can I help you?" I reply, "No, I just had a moment of hesitation where I couldn't decide if I should get my coffee, or go back out to my car where I left my laptop." The stranger replies, "It sounds like you need the coffee," chuckling as she walks off. She rounds the corner and is now out of sight. I notice a laptop sitting unattended on a conference table in a nearby room. I walk in, disconnect the power cable, quickly place the laptop in my bag and walk to the exit, all in less than 15 seconds. Trying to walk casually is hard when one's heart is beating so hard, but I try anyway as I return to my car. Checking my phone as I walk, I see my team has already started to find network assets and vulnerabilities from the Pwn Plug. This has been a smashing success!

At this point this story could go in two different directions. If a black hat attacker were behind this, they would review the stolen documents and laptop, remotely exploit internal assets via the Pwn Plug, and over the next few months slowly ex-filtrate sensitive data, selling it to the highest bidder. But in this case it was not a black hat. Instead, it was a white hat, thus the post-exploitation workflow is significantly different. First, the white hat immediately contacted the client to inform her that the test was successful. A meeting was set up where the infiltration team shared preliminary findings and the laptop was returned. Upon returning home, the next few days are spent performing network penetration through the Pwn Plug, followed by about a week of documentation and report writing. Report writing, while less exciting, is arguably one of the most important things the infiltration team does. Everything done during testing matters only if it's well documented and communicated in an understandable manner.

Perhaps the most interesting element of this story is that the person leading this white hat attack against a Fortune 100 company was a student sitting in a US MIS program three years ago! The remainder of this paper details the demand for IT security experts and then suggests topics that will help MIS students prepare for opportunities such as those enjoyed by our co-author, a professional from the corporate world.

2. STRONG INDUSTRY DEMAND

The scenario described above could have been taken from a script for a spy movie, but actually quietly plays out countless times each day by IT security professionals. These professionals are hired by the world's largest companies to test network security, which is increasingly becoming an important part of the audit process. For years the issue of information systems security was isolated to network administrators and other technical staff. However, the issue has recently found its way into the boardrooms of the world's most sophisticated corporations as well as the highest levels of government.

Every week brings new disclosures of corporations and governmental agencies being hacked. The public is often surprised that the victims of these cyber attacks are some of the most sophisticated companies in the world, including Apple, LinkedIn and Coca-Cola. It is a common refrain amongst IT security professionals that there are two types of companies that have been hacked: those who know they have been hacked and those who have been hacked but are not aware of the attack. These transgressions are particularly troubling because the attackers are often seeking a component of a firm's competitive advantage -- its intellectual property. Hackers are not only interested in pilfering intellectual property, however. In the case of Coca-Cola, it appears the hackers were focused on learning the company's tactics and plans related to the acquisition of a major Chinese company called Chinese Huiyuan Juice Group (Elgin, Lawrence and Riley 2012).

In addition to private sector hacking incidents, governments across the globe are increasingly the focus of digital attacks. It is now a fact of modern civic life that the ubiquitous digital networks underpinning almost every aspect of governmental operations are being targeted by various groups. The motivations for these attacks range from social protests, such as those surrounding WikiLeaks founder Julian Assange's arrest, to fully-supported government initiatives. Case in point: it was recently discovered that a unit of the Chinese military was responsible for many of the cyber attacks on American governmental agencies and US-based global corporations (Sanger, Barboza and Perlroth 2013). In response to this, President Obama recently issued an executive order requiring companies responsible for the operation of important parts of our national infrastructure, such as the electric grid, to meet high security standards (Gorman 2013). Clearly, issues surrounding governmental cyber security will occupy nations around the globe for years to come.

The cyber security challenges facing corporations and governments have caused an explosion in demand for security experts (Smith 2013). In fact, the unemployment rate for IT security specialists is estimated to be around 3% (Chabrow 2013). It is estimated that government needs 10,000 experts while the private sector has an immediate demand for 40,000 IT security professionals (Fitzpatrick 2012). Accordingly, it is our view that university-based MIS programs are in a unique position to help fill the tremendous demand for IT security specialists. In order to capitalize on this opportunity we encourage MIS faculty to take a fresh look at curriculum issues and match industry realities to university classroom activities. In the next section we suggest topics that might complement the development of a cyber security course. The basic technical skills contained therein, along with non-technical topics, will help our students take advantage of the opportunities that exist in this industry. The execution of the requisite tasks relies on a dynamic, broad, and difficult education, and currently, there is a significant shortage of qualified entrants into the industry.

3. SUGGESTED CURRICULUM TOPICS

The following topics provide a good foundation for undergraduate MIS students interested in pursuing IT security positions. The general outline is the by-product of our experience. We also reached out to the IT security community through Reddit and received positive and productive comments; this input resulted in our team identifying these topics that will allow students exposed to them to be able to enter the field and contribute to the management and maintenance of an information security program. In addition to the suggested subject areas, it is assumed the courses focused on IT security will foster technical writing skills, social skills, team skills and presentation skills. It should be noted that IT certifications are currently the best measure the industry has for regulating competency, thus academic programs should work to integrate respected certifications such as the CompTIA Security+, CCENT, and GIAC G2700 certifications.

Linux and Windows Fundamentals:
At minimum, students should have a working understanding of the Linux and Windows operating environments. This includes comfort with the Linux and Windows command line structure and environment, and the ability to script basic tasks. We suggest students interested in this area be exposed to Ruby and Python.

Networking:
Students will learn the basics of networking and network security tools. At a minimum, students should have a good understanding of Active Directory-based networks, including how resources are authorized and shared in a domain environment. This includes a thorough understanding of the TCP/IP and OSI networking models and the fundamentals of IPv4 addressing and routing.

Legal Regulations:
Due to the nature of the industry, students should be aware of the relevant legal code and federal and industry regulations surrounding their profession. This class should include a discussion of security requirements for various security clearances. This is particularly important as private sector contractors are often required to possess security clearances. Exploring this topic might provide an opportunity to bring in colleagues from the law school and legal community to share current advances in legal and law enforcement circles.

Computer Forensics and Incident Response:
Students will learn electronic evidence collection methods, incident response techniques, and basic analysis techniques. Students should be exposed to the investigative project process as well as industry best standards. The SANS organization has excellent community resources to support this.

Cryptography:
Students will learn basic cryptography ideas and their real world implementations. It is important for students to understand secure systems of communication and have a working knowledge for implementation. Students will learn common cryptographic terms, systems, and popular implementations of cryptographic principles, such as public-key cryptography. The Coursera course on cryptography has excellent resources that can be incorporated into lectures and projects.

Information Security Governance and Risk Management:
The majority of security testing is driven by federal and industry-specific standards. Students should have in-depth knowledge of the major frameworks (NIST, ISO), and be aware of the various industry frameworks (PCI, GLBA, SOX, HIPPA, GLBA). Students would be encouraged to pursue the GIAC G2700 certification, the gold standard in this area.

Security Engineering:
Students will learn how to engineer an environment that reflects physical security and IT security. This is particularly important because many firms have significant deficiencies

related to poor physical security practices. In addition to standard issues such as access control, identity management, and physical security, students should be exposed to business continuity and disaster recovery planning. All students should have experience creating disaster recovery planning documents.

Information Systems Security:
Students will learn how to engineer a secure computing infrastructure. Network and system security principles will be taught with emphasis on defense-in-depth. Students will also learn system maintenance, system monitoring, and audit log analysis techniques. Class discussion should include current threats and vulnerabilities, and methods for mitigating "zero day" attacks.

Penetration Testing:
Students will learn, use, and create tools to perform lab-based penetration tests, and will write reports and executive documents based on their findings. The class should also include a capture-the-flag contest and red-team versus blue-team exercises.

Soft Skills, Social Engineering:
Students will gain exposure to a number of soft skills required to be effective in a business setting. These skills include interpersonal communication, performing client interviews, and more, which all integrate well with the practice of social engineering. Students should be comfortable with social engineering techniques like physical social engineering, email social engineering, and social engineering over the phone. They will also learn ID badge replication, lock picking, and other general social engineering skills.

Current Events:
While it is easy to focus on the technical and managerial elements of the IT security professional, it is important to be familiar and conversant in current events. This is an industry that is embedded in a world changing at an extraordinary clip. Further, the rich real world environment in which security experts operate brings relevance and context into the classroom, thereby enriching the academic environment. One strategy we have employed effectively is to have students present on current events at the beginning of every class.

Ethics:
Our last topic is arguably the most important. It is clear that the powerful systems and technologies surrounding the IT security field are taking us into new ground. Because of this, it is incredibly important that students be engaged in robust, timely debates and discussions around ethics and values. As a matter of course, IT security professionals wield tremendous power and often have access to the most sensitive corporate and personal data imaginable. Accordingly, the men and women pursuing careers in IT security should be exposed to ethics across their entire MIS education.

4. CONCLUSION

The aim of this paper has been to illuminate an exciting but little-known component of the IT security field. One of the challenges MIS academicians often face is conveying to students the breadth of opportunities within the MIS field and then providing insight into what an actual day might look like. When we tell stories similar to that found in our introduction, with all the excitement and challenges associated with the work in which some security professionals regularly participate, it invariably piques significant interest. However, there is a mismatch, and at times, a lack of understanding, regarding the skills required to pursue these opportunities. It is our hope that the topics outlined in this paper can help faculty develop and justify courses that will help prepare students for this field.

Besides primarily promoting the terrific opportunities enjoyed by IT security specialists, we also encourage the MIS discipline to creatively rethink how topics related to IT security and ethics can be cultivated across the entire curriculum. It is our position that the general IT security literacy of all business school students needs to be considered and advanced. The implications and threats posed by IT security breaches are obvious and at the fore of public and private sector governance. Moreover, the technologies that sit at the center of our organizations are also wholly integrated into our personal lives. In the private realm, security breaches and violations have the potential to trample on the most intimate aspects of our lives (Eder and Valentino-DeVries 2012). MIS faculty have a unique opportunity to expose students to these issues and to teach them steps to take to protect themselves as well as the organizations they will be leading from these types of intrusions.

We would also suggest that MIS faculty think beyond producing IT security specialists drawn solely from the general undergraduate and graduate student populations. We believe MIS academicians can make a substantial contribution to the active executive population through the development of executive education courses surrounding IT security topics. It is a widely-held view that many senior members of management, as well as corporate boards, lack understanding and expertise in cyber security issues (Chabrow 2013). Many schools have executive education programs; these forums could provide the opportunity for MIS faculty to partner with industry professionals to work side-by-side in teaching and conveying ideas around this timely topic.

Finally, we submit that universities are the ideal place to provide this foundational training. MIS students are well suited to take advantage of these opportunities. An MIS education invariably exposes students to the general business curriculum where they receive a good foundation in the major business domains, which is extraordinarily helpful in IT security work. This broad-based business education, coupled with deeper technical skills such as those outlined in this paper, provide an ideal background for successful entry into the field. However, we suggest there is another reason why MIS students are exceptionally suited for these opportunities, and that is the liberal arts education that is part of the pursuit of a college degree. While exposure to the

technical and organizational topics we provide our students is invaluable, the big questions advanced by our humanities colleagues also play an important role.

Our society will be better served if thoughtful, well-educated men and women pursue the sensitive and important profession of IT security. MIS academicians have the opportunity and obligation to contribute to this critical enterprise.

5. REFERENCES

Chabrow, E. (2013a, January 5). 3% Unemployment Among Infosec Pros? Bank Info Security. Retrieved February 22, 2013, from http://www.bankinfosecurity.com/blogs/3-unemployment-among-infosec-pros-p-1400

Chabrow, E. (2013b, January 9). Security Skills Shortage Places IT at Risk. Bank Info Security. Retrieved February 22, 2013, from http://www.bankinfosecurity.com/skills-shortage-places-at-risk-a-5409

Eder, S., & Valentino-DeVries, J. (2012, October 6). A Spy-Gear Arms Race Transforms the Modern Divorce. Wall Street Journal. Retrieved from http://professional.wsj.com/article/SB10000872396390443995604578002751421246848.html

Elgin, B., Lawrence, D., & Riley, M. (2012, November 4). Coke Gets Hacked And Doesn't Tell Anyone. Bloomberg. Retrieved February 22, 2013, from http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html

Fitzpatrick, A. (2012, May 29). Cybersecurity experts needed to meet growing demand. Washington Post. Retrieved from http://articles.washingtonpost.com/2012-05-29/business/35458606_1_cybersecurity-college-students-visit-colleges

Gorman, S. (2013, February 13). Obama Presses Cybersecurity Effort. Wall Street Journal. Retrieved from http://online.wsj.com/article/SB10001424127887324432004578302463635305972.html

Sanger, D., Barboza, D., & Perlroth, N. (2013, February 18). China's Army Is Seen as Tied to Hacking Against U.S. The New York Times. Retrieved from http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

Smith, G. (2013, January 28). Pentagon Cyber Force Turns To Hackers To Meet Growing Demand. Huffington Post. Retrieved February 22, 2013, from http://www.huffingtonpost.com/2013/01/28/pentagon-cyber-force_n_2567564.html

AUTHOR BIOGRAPHIES

Eric Fulton is a specialist in network penetration testing and

web application assessments. His clients have included numerous Fortune 100 companies, international financial institutions, global insurance firms, government entities, telecommunications companies, as well as world-renowned academic and cultural institutions. Eric has spoken at the global hacker conference Defcon, taught at the prestigious Blackhat Conference, and has spoken at numerous community events. Recently, Eric founded SubSector Solutions, a world-class information security company based in Bozeman Montana. Eric contracts with a diverse range of companies and governments, presents bleeding edge research at national and international conferences, and creates game-changing technologies through advanced research. In his free time Eric enjoys the Montana outdoors and lobbies for increased privacy legislation.

Cameron Lawrence, Ph.D., holds a Ph.D. from the

London School of Economics in Information Systems and teaches in the School of Business at the University of Montana. His research has been published in academic work has been published in some of the leading international journals in the field of Management Information Systems including the European Journal of Information Systems, Communications of the Association for Information Systems and the Journal of Information Technology Theory and Application. In addition, he has been selected as the Outstanding MIS Faculty member five times and was recently awarded with the prestigious John Ruffatto Memorial Award, which recognizes excellence in the classroom across the University of Montana system.

Shawn Clouse, Ed.D. is an Associate Professor of

Management Information Systems (MIS) in the School of Business Administration at the University of Montana. He earned an MBA from the University of Montana in 1990 and his doctorate in Higher Education and Technology Leadership from the University of Montana in 2001. Shawn completed a Post-Doc in MIS at Washington State University. He teaches courses on networking, e-Commerce, project management, systems analysis & design, and multimedia development. His research interests include information privacy, website

usability, utilizing technology for teaching and learning, and the technology issues related to e-Commerce and business processes.

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096