"It's all about people, process, and technology. Technology is dead last in the order of importance when it comes to security."

The recent and explosive growth of the Internet and technology has brought many good things such as e-commerce, collaborative computing, online markets and new avenues of sharing and distributing information. But each side has its counterpart, and with the technological advances came hackers. With this dark side and the many security breaches that are associated with it, companies, governments and individuals are afraid of hackers breaking into their servers or networks, stealing valuable data, collecting passwords and intercepting financial and credit card information.

And many times this can become reality. Recently, there has been a flurry of security breaches among large organizations such as Western Union, that reported a security breach on their Web site that let loose the credit-and debit-card information for 15,700 customers. Another recent hacker case is a 16-year-old youth, who admitted hacking into military and NASA computer networks. His activities caused a three-week shutdown of NASA's systems and a security breach of a military computer network which protects against conventional, biological, chemical and nuclear-weapon attacks. That's just a small sampling of actual hacks. Most industry watchers agree that only a handful of security breaches are ever reported.

For a long time, most computer network crackers hacked a system for the same reason: "Because it's there." But that's no longer the only reason or even the dominant one. More hackers now do it because "It's where the money is." In the past decade, hackers have changed from script kiddies who hacked websites and spread worms to professionals sponsored by foreign governments and organized crime. Modern hackers want more than infamy. They exploit new technologies to crack systems or hack into computer systems and hold data for ransom. Hackers today commit real crimes, sometimes for significant financial gain.

To safeguard themselves from the modern hackers, most companies and government agencies that want to uncover network and system security vulnerabilities have two choices: They can hire a team of penetration experts to scan and probe their systems and uncover their vulnerabilities, or they can wait for a malicious hacker to come by and exploit them. Unfortunately, many times it is the latter. Instead a security analysis or penetration test, performed by a security consultant, would produce a report or security posture assessment, detailing all vulnerabilities found and the actions needed to remedy them and minimize the risk of being the victim of a successful hack attack.

The security consultant or penetration expert can be a "white hacker", someone who uses ethical hacking to discover vulnerabilities within a network or a reformed "black hacker", who once was an active part of the dark side and used to exploit the identified security holes. The subject of whether it is ethical to use former hackers to evaluate a network's security is a topic that is often hotly debated. This article explores the pros and cons of using former hackers in such roles as well as as ethical hackers, their skills, attitudes, and how they go about helping their customers find and plug up security holes.

Ethical hackers or security consultants typically have very strong programming and computer networking skills and have been in the computer and networking business for several years. Their base knowledge and expertise is augmented with detailed knowledge of the hardware and software, project management skills and methodology which are necessary for the actual vulnerability testing, as well as when reporting after the test was performed. In addition to that, ethical hacking seminars, courses and certifications are being offered to IT professional to broaden their horizon and skills in these fields. But many times these hacking courses and seminars only provide a very limited insight, outdated hacking or only basic hacking techniques. Their main purpose is to educate professionals but not to create a new generation of hackers. The goal is to fill security holes, not exploit them.

A disadvantage that white hackers or security consultants have over hackers is the real world experience and the insight knowledge. There are many things that cannot be tought in a seminar or learned from a book. The most obvious advantage former hackers have, is the real world hacking experience. As each network system differs based on various network defenses, the hack approch will be unique and only someone with plenty of real world hacking experience can efficiently go from using one technique to another as required by the present situation.

Another positive aspect of hiring reformed hackers as security consultants is that stayong up on the latest security explits, vulnerabilities and countermeasures is part of their job. A good hacker has a level of security knowledge that goes far beyond that of most other IT professionals. Keeping up with the latest exploits and countermeasures is a full time job and although the IT professional has an acceptable level of security knowledge, they must focus most of their attention on the day to day responsibilities of keeping the network up and running. To make up these "defficiencies" many white hackers and security consultants rely on automated and commercial vulnerability and penetration software, that can provide needed security reports, but their functions are limited. The huge differences can be seen when comparing the results from an automated scan and a hacker assessment.

But before a company makes the decision to hire a reformed hacker, one needs to evaluate the negative sides. Certainly there are several types of hackers that can be found. One kind oft them are the "gray hats" - the unpaid tinkerers who find flaws to improve security for everyone. They are the best hackers, because their passion for tinkering drives their excellence and they do not break the laws. The black hat hackers - the criminals - break the law and feel justified doing it. They are the kind of hackers who seek to increase their fame in the hacker community, while others want to prove at any cost that their targets' security is vulnerable. Black hats wreak havoc not only by their own actions but also by drawing attention to weaknesses that they and cybercriminals can exploit. The last and worst kinds of hackers are the cybercriminals, who perpetrate the worst crimes. They are paid to use existing tools and techniques to steal confidential personal, government or industry information, and particularly financial data. Cybercriminals usually work for foreign governments, organized crime or independently.

The probably biggest negative in the decision making process is trust. Which hacker will you hire and how much can you trust them? The main premise of security is deciding who you trust and then locking out everyone else. When hiring a hacker as a security consultant, because of network's security concerns, paradoxically the trust goes to the crimial. Not only is it the trust factor but also the impact this decision might have on the customers and shareholder. How will the customners react, if they knew a former criminal was hired to test the security of a system or database that contacins all personal and financial information? Someone with a questionalble morale and judgment, is not someone who should have control of a corporate network with sensitive data. In most cases hackers, and that is what makes them hackers, do not appreciate or respect standard business processes and structures. A disgruntled hacker with inside knowledge of a company's networks could create a nightmare scenario.

Hackers are like adventurers, motivated by intellectual curoisity."The more secure you make your systems, the more you attract them. The hacker mind-set is like exploring space, except they're exploring the network." If that essential curiosity on finding out how things work, which is what causes people to be hackers, goes away, then you don't necessarily want that person as a hacker or security consultant. However, just because a hacker has the desire and capabilities to explore a network, does not necessarily make them prepared to build a secure network and fix identified vulnerabilities. Breaking into things, does not always mean knowing how to fix them. These are two different skill sets. Once security threats have been identified, these need to be communicated including the potential business processes affected by the vulnerability, along with a list of impact assessments and countermeasures. Besides technical knowledge, the hacker will need to have experience in business processes and management, to relay his findings to the company.

Another hey factor to consider before making a decision who to hire as a security consultant, is to know that no computer system is ever completely secure, espcially when considering the human factor. Spending astronomical amounts of money pursuing total security, by hiring security consultants and eventually becoming dependent on them, is not going to help. Some corporations in some industries must guard against intrusions from tech-hungry foreign governments - in particular China, France, Israel, Japan, Germany and Russia - that converted their cold-war spy machinery into "economic espionage" units but that does not apply to all businesses A realistic set of goals of what to expect from a security consultant need to be set first.

But no matter what the decision is and if the company hires a professional security consultant or a reformed hacker, the real threat will be still there. Any hacker, who wants to exploit a system will always try to use the path of least resistance. This path of least resistance is often through the front door, said Paul Proctor, research vice president of security and risk at Gartner. The front to door can be "identified" as the area over which businesses may have the least control: people. People are the weakest but first link when it comes to security. With good social engineering skills and not very well trained employees, disgruntled workers and ex-employees, a hacker can get enough information to access a system, insert malicious codes that contain keystroke and network sniffers and other means to collect information. The hacker just "exchanged" his keyboard with social engineering. And this is a part of security where a highly educated security consultant or a reformed hacker will not be able to help you.

By Dasha Deckwerth
Stealth - International Intelligence Security Service Inc.
www.stealth-iss.com

About Stealth - ISS® Inc.
Stealth - ISS®, headquartered in Tampa, FL., is a privately owned Information Technology security consulting company with main focus on regulatory compliance, security integration, security consulting and managed security services for both government and commercial customers.
Founded in 2002, the company has earned an outstanding reputation for professional security services including vulnerability assessments and regulatory compliance such as Sarbanes-Oxley, HIPAA, NIST and ISO standards. Stealth – ISS® also recently expanded its data center services providing faster and secure hosting and colocation solutions for customers worldwide.
Stealth - ISS® has partnerships with several leading manufacturers of various security applications and products and was awarded the NATO BOA agreement in 2003.

About the Author
Dasha Deckwerth is the CEO at Stealth - ISS, with extensive experience in international business and computer security. Prior to her position as CEO, Dasha had gained extensive international business experience in various European, Asian and Central American countries and later became the VP of Marketing and Business Development at Stealth - ISS® in Berlin, Germany. She also worked on several projects as security and regulatory compliance consultant in the commercial sector as well as for various NATO countries and government agencies. Dasha's current focus includes managed data center services, knowledge management, regulatory compliance applications and services and security implementations and consulting. Mrs. Deckwerth holds a B.A. in International Relations and Foreign Affairs from Eckerd College, is currently pursuing an MBA in IT Management from Touro University and speaks six languages.