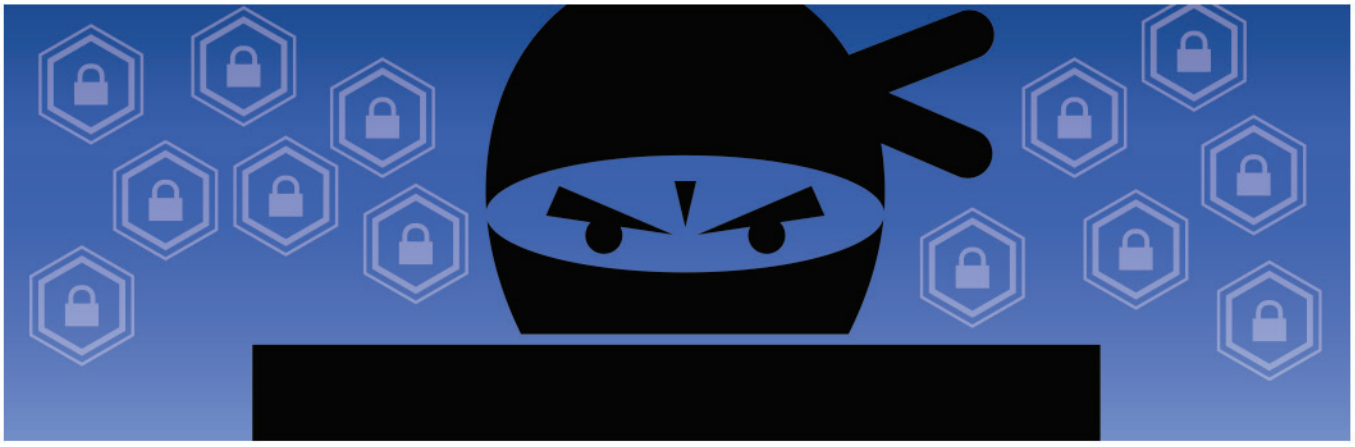
First Cybersecurity
Information Series



The HIT Cybersecurity Battleground

Using Education, Training and Certification to Help Healthcare Entities Fight Back

First Healthcare Advisory Solutions

The HIT Cybersecurity Battleground

Using Education, Training and Certification to Help Healthcare Entities Fight Back

February, 2016

The Office for Civil Rights website reports that data breaches in healthcare totaled over 112 million records in 2015. As if this were not enough to keep Healthcare Executives up at night, a new attack vector has now arrived on the scene: Ransomware. CEO Allen Stefanek recently reported that Hollywood Presbyterian Medical Center paid hackers $17,000 to restore operation of their computer networks after a ransomware attack shut down their computers. As banks and retailers have shored up their security, hackers have turned to the less-secure healthcare sector.

When it comes to information technology, there is a saying: "The only constant is change." With Moore's Law describing the doubling of computing power every two years, and Rock's law stating that the cost to keep up with increased computing power increases exponentially; it is no wonder that organizations struggle to stay current without breaking the bank. Within the information security domain of IT, this struggle to keep up is exacerbated by the half-life of information security knowledge. According to G. Mark's law, "half of what you know about information security will be obsolete in 18 months." Most healthcare IT departments have begun to organize themselves and are investing heavily in hardware appliances and software, with the understanding that the only way to truly to catch up, and stay caught up, is to invest in the continuing education of all employees and the staff employed to operate the cyber-defense tools they have invested in. The human element has caused the need for cybersecurity, and the human element is required to combat it. As computers and computer networking hardware were first being built, little thought was given to the need to keep information safe. One day a curious human decided to see what information they could dig up on a system and computer hacking was born. For a long time hacking was the realm of the intellectually curious human or the "script kiddies" who just wanted to see what pranks they could pull off. Then world of computing and hacking changed forever in 1988 when Cornell graduate student, Robert Morris, created and launched his worm from MIT's campus on November 2nd.

After Morris' unintended demonstration, the practice of hacking grew out of humanity's dark side and malicious behavior took center stage with website defacements, posting of obscenities, and denials of service running rampant. Soon organized crime and nation-states joined in on the dark side changing what started as a game for script kiddies to full scale economic warfare. In a recent interview, Marc Goodman confirmed this assertion: "The old image of a hacker was 17-year-old kids living in their parents' basements. Today, the average age of a cybercriminal is 35, and 80% of black-hat (e.g., criminal) hackers are affiliated with organized crime."

While some may dispute the statement that 80% of hackers are associated with organized crime, there is no disputing the fact that black-hat hacking is a

sophisticated and organized industry today. Jim Anderson, at BAE systems has stated, “There are websites where a new thief can essentially buy a ‘starter kit’ that includes malicious code that rookies can use in their first attempts at criminal behavior.” He goes on to state that there is “no disorganized digital crime. Because of the way criminals have organized, the threat landscape is ever evolving and more importantly, ever growing.” There are black markets for a wide variety of malicious services and value-added resellers at every step in the chain to take economic advantage of hacking activities. Most importantly Anderson states that part of the evolution of organization is information sharing. “The rate at which information is shared among the criminal element means that an attack at, for example, one bank, could be replicated by multiple bad actors at financial institutions globally within moments.”

It is the ever-evolving, information-sharing nature of the dark side that is of utmost concern to the informed healthcare firms that are best protecting their operations. They recognize that investments in information security infrastructure are necessary but insufficient. Quoting Dr. Eric Cole, “prevention is ideal, but detection is a must.” Take the case of antivirus software as a simple example. Most every laptop in the world runs antivirus programming, yet antivirus software vendors are taking it on the chin these days. All a malicious attacker has to do is change the “signature” of their virus slightly to make it unrecognizable to the library of signatures on file with the antivirus firm, and their new virus easily slips through defenses. Vendors are spending a fortune to keep up and at times are forced to send out daily updates to keep their products relevant in the struggle to defend against attacks. If you asked a group of security experts today whether they use antivirus or not, a significant portion of them would answer that they do not.

While Gartner analyst Ruggero Contu feels that antivirus has some value, he points a direction towards today’s new required investment: “Not to have malware protection would be foolish,” he says, “but spending money on learning how attackers are working, and changing your business to thwart common attack techniques may be a better investment.”

Learning how attackers are working and developing tactics to thwart them is the cornerstone philosophy of the SANS Institute. “Offense informs defense” is the basis of the continuing education and degree program offerings of SANS. One of the most popular courses at the institute features “Ethical Hacking” as its primary subject. In this class, students are given access to the latest tools and techniques being used by the Black Hat community. SANS believes that learning how attacks are organized helps a defender organize the appropriate response. Having equipped their operations with a suite of hardware and software tools, healthcare organizations recognize that educating their workforce and stimulating their in-house knowledge with the latest mitigation tactics is imperative.

First Health Advisory Solutions recognizes the fact that continuing education of the workforce employed in HIT cybersecurity is the only way to organize a defense against evolving malicious activity. Recognizing the need for continuing education, First has partnered with the SANS Technology Institute. Through this partnership, First’s team of advisors and employees have access to the latest learning in both offensive and defensive information security practices and are better equipped to advise their healthcare clients facing ever increasing security demands.

First

Healthcare
Advisory
Solutions

Contact First

Please Contact:

Kerri Gallagher
484-667-7426
kgallagher@fcp.com
www.fcp.com