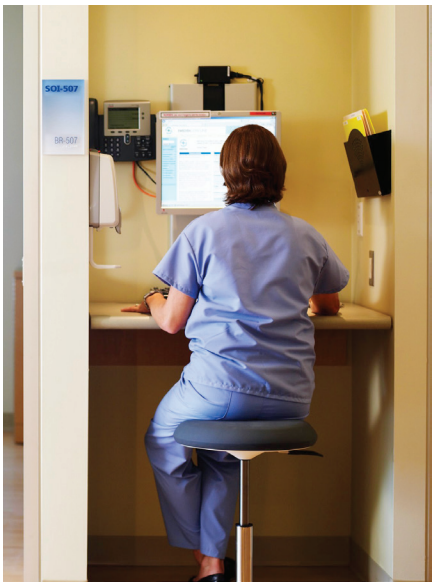
THE CYBER THREAT TO HEALTHCARE

According to the The Washington Post, there are "gaping security holes" in many of the systems that hold our healthcare data".

"A physical server drive containing 1.9 million patient records was stolen...."

"....More than 21,000 patients have been impacted by a trio of recent healthcare data breaches throughout the U.S."



Healthcare is undergoing a fundamental transformation in the way that the industry operates and does business. This is equally true for healthcare payers, providers and life sciences organizations. Growing regulatory requirements for payers and providers to move to electronic medical records, new coding, telehealth and telemedicine, and secure electronic communications is combining with downward price pressure from government, insurance and consumers to force all aspects of healthcare to be leaner and more efficient while at the same time more secure. "Do more with less", is the message coming from all sides.

At the same time, the pharmaceutical industry is coming under increasing pressure as lucrative US and European patents expire, or are ignored by generic manufacturers overseas, often with the support or blessing of their national governments and legal systems. The practice of 're-formulation' or 're-branding' of patents has essentially been killed off by the courts. What compounds this is that most national governments are forcing down drug prices anyway they can, thus eating into profits and Research and Development funds of manufacturers.

There has also been a major change in the risks that the healthcare industry faces outside of the usual malpractice, malfeasance or the fact that someone slipped on a freshly mopped hospital floor! There has been a truly dramatic rise in the cyber risk over the past few years. If you didn't realize it, this cybersecurity risk now out-weights all other risks **combined** to the Healthcare industry!

Cyber Theft

The cybersecurity threat has never been greater and continues to grow exponentially. What was once the realm of teenage hackers intent on showing that they were smarter than the generation above them, is now very different. In only a few short years cyber criminals intent on monetizing the sale of stolen data have created an open market for business critical information on the Internet. Cybercrime is now a recognized, and in some nation states, even 'legitimate', business.

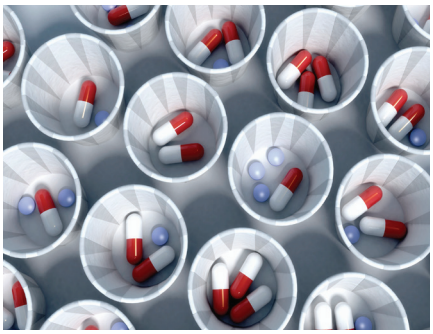
One of the biggest perpetrators of cybercrime is even traded on the Russian Stock Market!

These organized cybercrime corporations now vastly outnumber the 'script kiddies' and 'political hactivists'. They simply keep their heads down and go about their business. They are even organized into separate companies. I use the collective noun of 'companies' rather than 'gangs', because that's the way many see them in other countries, and usually the way they see themselves. These people wear suits to work!

According to the Ponemon Institute Third Annual Benchmark Study on Patient Privacy and Data Security, of 80 healthcare organizations surveyed nearly all indicated they had at least one data breach in the past two years. 45 percent have had more than five incidents.

A recently published Wired article hypothesized that as health data increasingly is pushed online, hacking becomes less a question of "if" and more a question of "when".

"What happened to Google Health? Gone! They didn't want the liability,"



One such 'company' will create code exploits to get past your security systems and sell these exploits to other companies who will then hack your systems and steal your data. They in turn, will then sell your data to other companies who parse and exploit the data, selling it off piece by piece based upon data type – Intellectual property, business intelligence, research and development, personally identifiable information, personal health information, financial and accounting data, etc.

This traded information is then used by other cyber criminals to sell your HR, customer or patient records to identity thieves, or exploit your finance systems by transferring your payroll out of the country, just as one team or 'company' recently did at a small hospital system in Washington State taking with it their million-dollar payroll.

We in the western world are just so trusting we have NO IDEA that anyone would want to wreak such havoc on our services for the elderly, the sick and our newborns! That they would want to steal and exploit our patient health or other data for their own abhorrent purposes! We fail to recognize that we are in a truly connected global society and that others who've been subject to 60 or more years of political oppression don't operate on the same moral code that we hold dear! More about that later.

Cyber Hactivists

If hacking for theft and commercial exploitation makes sense to common criminals, it stands to reason that theft of embarrassing information or defacement of web sites owned by those with whom they disagree would make sense to political activists. The rise of organized groups such as 'Anonymous' and 'LulzSec' and the multitude of other politically motivated hackers continue to attract news headlines.

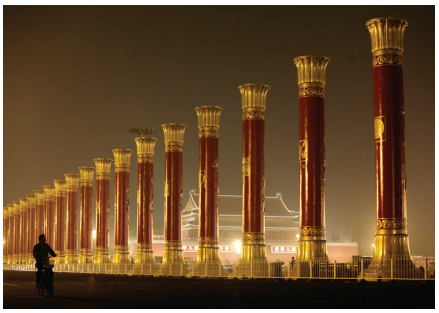
Although we have yet to see wide scale political cyber attack on healthcare delivery, several pharmaceutical companies have been the subject of some major attacks. What is more important is that these groups focus on attacking the fabric of societal information security. Take for example the recent large scale attack on RSA, which although not a direct attack on healthcare, created weaknesses and security exploits that could then be further exploited by others for nefarious purposes.

Cyber Espionage

What makes the cybersecurity risk all the more worrying is the rise of Cyber Espionage. State sponsored military intelligence units hack the systems of friendly and non-friendly governments, defense contractors and more recently commercial businesses. They do it in order to steal intellectual property or business intelligence to position their nation's emerging industries with the best possible competitive advantages alongside their global counterparts, most of whom have spent decades and invested hundreds of millions of dollars getting where they are today.

Within a mere five years, the Peoples Republic of China fully expects to be on an even par with the United States and Europe in most of its scientific industries including healthcare life sciences. Not as a result of some herculean national effort, but largely by the exfiltration intellectual property from leading global companies.

Many of the formulas for the next era of pharmaceuticals are already in the hands of new Chinese Corporations stood up by the government there, or by units of the Peoples' Liberation Army (PLA) who own or have an interest in many, if not most, of China's new corporations. Interns gaining job experience while at American or European universities take back to China the skills, proprietary processes and procedures needed to manufacture these drugs,



Ponemon found a shortage of technologies, funding and security expertise at many organizations. Only 27 percent of organizations in the study said they have sufficient resources, and 34 percent said they have a sufficient security budget.

Ponemon found that a major challenge for IT security is the increase in criminal attacks, which has risen from 20 percent in 2010 to 33 percent in 2012.

Insider negligence was the biggest cause of data breaches among the 80 firms studied by Ponemon

The Regional Medical Center in Memphis is notifying patients of a HIPAA breach after an employee sent out three unsecure emails containing the protected health information and Social Security numbers of nearly 1,200 patients. The unsecured emails included patients' names, Social Security numbers, dates of birth, account numbers, phone numbers and outpatient physical therapy services data.

A hard drive containing data of 5,418 patients stolen from Kentucky hospital. Hospital officials reported that the information on the hard drive was not encrypted, but was maintained in a locked, non-public, private area.

while PLA Cyber Espionage Units, such as the group known as 'APT1' or 'Unit 63198' of the PLA's 3rd Department, steal the latest medical, pharmaceutical, and biogenetic breakthroughs. Other industries are in similar situations - and that breaking new experimental medical procedure that you hope to one day publish, is already published on the other side of the world.....in Chinese, thanks to your research notes which were obtained from your PC not long after you wrote them!

The gloves are off. This is the current and future business model in which cyber espionage is just one of many tools in the toolbox of a new order.
Welcome to a global cyber economy, an increasingly fickle workforce and the growing difficulty in maintaining business ethics at both the employee and employer level. The old paradigm of a 'job for life' is long gone and US public companies are now very adept at shedding 20-year veterans without cause, simply in order to boost quarterly earnings figures!

So too are employees learning not to trust their employer and will change jobs for nothing more than a one-time signing bonus. As for turning down a monetary offer for corporate secrets or the keys to the company; with the decline in loyalty on both sides, this is something that can no longer be assured. The steadfast global corporations of the past have dug themselves a hole and their best defense against cyber attack, their people, can no longer be relied upon to protect the corporate empire! Even those motivated to protect their company are ill equipped to do so, against ever-sophisticated attacks and without additional security awareness training, and tools. Companies also need modern day cybersecurity policies, standards, procedures, and guidelines with powerful and automated enforcement of security controls and processes.

It was only a few years ago after all, that a disgruntled employee held the City of San Francisco's network hostage – even after he was ordered by a judge to disclose the administrative credentials.

Cyber Terrorism

Although we have yet to see the effects of a concerted attack against the soft targets of healthcare, Cyber Terrorism is the third of the risks facing this industry. Many of our healthcare systems are wide-open and are easy pickings for the likes of Cyber Terrorists. It would be incredibly easy for a cyber terrorist to hold a hospital, or health provider to ransom on little more than the threat that they 'own' that hospital's IT systems and could universally change the dosage on all IV pumps, or remotely control other medical devices in order to inflict damage on soft targets, cripple life dependent systems in ICU or NICU, or simply put patients at risk by other means, perhaps through changing their prescriptions on EMR or pharmacy systems. Most medical devices or systems are ill protected against the kinds of concerted cyber threats that could be exerted against them. Most use old communication protocols that have known exploits and weaknesses and few if any would withstand an advanced persistent cyber attack.

Cyber Assassins

Cyber Assassins now have the ability to remotely control pace-makers, insulin pumps, or other electronic surgical implants of thousands of patients via little more than common 802.11 WiFi and a rudimentary knowledge of how to manipulate such a medical device. Many of these medical devices have open unsecured remote access for monitoring by doctors and other primary care practitioners and many still have the original unchanged default password setup by the manufacturer, if they have a password at all.

This could change the way 'hits' are ordered and conducted by organized crime against world leaders and other high value targets. An assassin could execute his crime in his car hundreds of yards away from a target with nothing more

"Appear weak when you are strong, and strong when you are weak."

"All warfare is based on deception."

"To know your Enemy, you must become your Enemy."

"The supreme art of war is to subdue the enemy without fighting."

-Sun Tzu, The Art of War.

then a high-powered antenna and a laptop! Who needs bullets and a gun, (perhaps a Walther PPK), when you have a computer and a little knowledge, most of which can be found easily on the Internet. It could be that we are entering the era of 'Cyber Assassin 00111' and leaving the era of 'James Bond 007' – both licensed to kill.

Cyber Warfare

As nation states struggle to protect themselves against cyber espionage and terrorism, so too do they need to prepare for and protect themselves against the threat of Cyber Warfare or Cyber Conflict.

The US and other prominent western nations realize their major systems have been penetrated or compromised and their critical defense and commercial secrets lost to cyber espionage. The need for the west to protect itself against these cyber warfare threats has never been greater.

The highly connected and technically advanced industrial nations are prime targets for terrorists and rouge nation states intent on inflicting serious harm or disruption on these countries. Currently that threat is most prevalent from the Peoples Republic of China, Iran, North Korea, many former Soviet states and emerging Middle Eastern powers such as the Syrian Electronic Army. Much of the critical infrastructure of the United States is already under attack – our power distribution systems, flight control systems, dams, water management and other supervisory control and data acquisition (SCADA), process control networks (PCN) and other Industrial Control Systems (ICS) are already targets. So too are our hospitals which use, or rely upon similar systems, technology and communications!

One only has to see the havoc raised by Hurricane Katrina on the New Orleans hospital system to realize that a widespread cyber attack on the hospital and critical care facilities of the United States or other developed nation, would result in the deaths of countless thousands of our most vulnerable citizens. A SCADA, PCN or ICS attack on hospitals to take out power, water, sewage, or air conditioning systems, would quickly render our hospitals incapable of caring for patients. Most would have to be evacuated to other unaffected facilities that have the capacity to absorb the patient load. In a Cyber War attack, the devastated or affected area could be too large to avoid loss of life.

Now imagine a man-made Katrina magnitude event that affected the entire continental United States. Where would patients go in such an event? There would be nowhere safe to evacuate and the fact of the matter is that our hospitals and other critical healthcare delivery facilities are largely unprotected and ill-prepared for cyber attack of any nature, let alone an organized and concerted attack on their critical infrastructure facilities.

Nearly all of the city of New Orleans hospital capacity was flooded within an hour of the dyke breaches, and most hospitals were unable to provide even basic patient services by the end of that day due to loss of water, power, sewer and other critical infrastructure facilities. None of the hospitals had adequate plans in the event of loss of critical systems and few were able to cope with the circumstances they found themselves in. All were eventually abandoned after trying their best to evacuate patients, but at the end of the week when help finally arrived 45 patients were found dead in their beds in largely empty hospitals.

Following the September 11, 2001 attacks, Mount Sinai NYU Health System lost a Data Center that handled clinical and business operations for three of the system's five hospitals, including NYU Downtown Hospital, three blocks from the World Trade Center.

During Super Storm Sandy, New York University-Langone Medical Center had to evacuate most of its neo-natal intensive care patients, because back-up electrical generators failed to operate as planned. The hospital needed over two

"Since about 2010, HHS has received over 600 breach notifications for almost 22.1 million health records."

"According to a recent Ponemon report, 94 percent of healthcare organizations have suffered a breach within the last two years. What's more, in the first quarter of 2013, breaches left 875,000 healthcare records exposed, according to American Medical News."

"According to Department of Health and Human Services (HHS), the majority (6 out of 10) of breaches in 2012 involved the theft of a hospital's unencrypted laptop. Three out of 10 involved employees or former employees downloading, emailing or inappropriately accessing patient information."

"The Indianapolis-based Cancer Care Group, announced in August 2012 that PHI for as many as 55,000 patients could have been compromised after a company laptop was stolen."

"Hollywood, Fla.-based Memorial Healthcare System, experienced a data breach involving nearly 10,000 patient records."

"Ponemon estimates that the average economic impact of data breaches over the past two years for healthcare totaled $2.4 million. Breaches costing more than $500,000 made up 57 percent of the healthcare organizations in the study."

"Medical files and billing and insurance records are the most likely to be lost or stolen, according to the Ponemon study findings. Lost or stolen payment details increased significantly, according to the study, rising from 17 percent in 2011 to 24 percent in 2012."

dozen ambulances to evacuate the infants and the support of many of New York City's over-stretched first responders.

The Veterans Administration has been fighting cyber attacks for a number of years. It became so bad that last year the VA had to remove a number of critical medical devices from its care facilities including glucometers, pharmacy dispensing, picture-archiving and communications systems. Seventy six thousand Veterans were affected.

The Rise in Data Breaches

Despite, or maybe as a result of, HITECH and the Omnibus HIPAA Rule, the number of reported cybersecurity breaches of Individually Identifiable Health Information (IIHI) or ePHI, continues to rise each month. And those are just the reported breaches. Figures suggest that between 70% and 80% of healthcare breaches go totally undetected by the healthcare entities tasked with protecting their patient data, largely because they lack the systems and expertise to recognize that they have been attacked in the first place!

The FBI has calculated that over 90% of hospitals have been attacked since 2002 which has cost the United States over $550 million annually in clean up costs and credit monitoring for those whose data was stolen.

Just recently the University of Florida had to notify over 5,600 patients and parents of its Pediatric Primary Care Clinic that that they should take appropriate measures to protect themselves from identity theft following the insider theft of patient records by an identity theft ring.

Based upon the magnitude of the problem, Health and Human Services (HHS) in its Omnibus update, has estimated that there will be 19,000 breach notifications from covered entities annually, affecting 6.71 million individuals – that's 1,583 a month, or over 50 per day!

In Memphis, Tenn., the Regional Medical Center (MED) issued a public notice on May 9, stating three e-mails were sent from October 2012 to February 2013 that included personal information of outpatient physical therapy patients receiving services between May 1, 2012, and January 31, 2012. The personal information included name, account number, date of birth, social security number, home phone number and type of service received. According to WREG, roughly 1,200 patients were impacted.

Indiana University Health Arnette in Lafayette, Ind., announced last week that an employee's password-protected laptop with patient information--including names, dates of birth, medical record numbers, diagnoses and dates of service--was stolen from a car in April. The organization indicated that it doesn't have reason to believe the information has been improperly accessed or used, but police were immediately notified, regardless. IU Health Arnett began mailing

Top 10 breaches for 2012

- ***Utah Department of Health - 780,000 records***
- ***Emory Healthcare - 315,000 records***
- ***S.C. Dept. of Health and Human Services - 228,435 records***
- ***Alere Home Monitoring, Inc. - 116,506 records***
- ***Memorial Healthcare System, Fla. - 102,153 records***
- ***Howard University Hospital - 66,601 records***
- ***Apria Healthcare - 65,700 records***
- ***University of Miami - 64,846 records***
- ***Safe Ride Services - 42,000 records***
- ***Medical Integration Services, Puerto Rico - 36,609 records***

According to a Ponemon report published March 2013, 94 percent of healthcare organizations have suffered a breach within the last two years. What's more, in the first quarter of 2013, breaches left 875,000 healthcare records exposed, according to American Medical News.

Thirty-nine percent of companies that had been breached said they still did not have a response plan in place, according to the survey, while just 19 percent said they had tools to determine the nature and cause of a breach.

According to Ponemon's study, of the 80 organizations analyzed, there was an average of 2,769 lost or stolen records per breach. Ponemon estimates the average cost per one lost or stolen record is $194. "Only one data breach could have an economic impact of about $537,186," the firm said.

Larry Ponemon, founder and president of the Ponemon Institute, said the average cost to the healthcare industry could potentially be as high as $7 billion annually.

According to the World Privacy Forum, a stolen medical identity has a street value of $50 today, compared to $14 – $18 for a credit card number complete with name, address and CCV2 number or $1 for a Social Security number.

"Lost backup tapes and CDs account for a large proportion of data breaches."

letters to affected patients--nearly 10,000, according to the Journal and Courier--informing them about the breach on May 10.

Presbyterian Anesthesia Associates in Charlotte, N.C., disclosed that a hacker broke into their website to access a database of personal information including names, contact information, dates of birth and credit card numbers for nearly 10,000 people, according to the Charlotte Observer.

University of Arkansas for Medical Sciences (UAMS) also recently notified 1,500 patients of a data breach that involved a resident physician who was terminated two years ago. UAMS discovered the resident keeping patient lists at the time, but somehow the files were still in the resident's possession following employment.

Is Healthcare Prepared for what's coming?

The short answer is no – not by a long shot! The Financial Services Industry has had 20 years to build the sophisticated anti-fraud systems it uses to minimize its losses through credit card and banking fraud. These systems are the backbone of its defense strategy against cyber criminals and other 21st Century cyber threats. Healthcare on the other hand, is just starting.

Until recently there was very little value in going after healthcare targets but over the past 12 months that has dramatically changed. In 2011 according to Bloomberg a credit card number traded on the Internet for $3.50. That same information today fetches less than a dollar thanks in part to improved anti-fraud systems of the banks and credit card processors.

With credit card numbers worth so little, cyber criminals are going after easier targets and healthcare is top of their list. Its systems are designed for patient care not protecting monetary assets, and cybersecurity is weak at best on the majority of clinical information systems. They were designed to operate in a closed loop, hospital-centric care model of the 1970's and 80s', - before personal computers, Windows, the Internet, or WiFi; before the advent of the electronic medical records, patient web portals, Health Information Exchanges, telehealth and telemedicine. What little security these systems had, was based upon the concept of 'security through obscurity' and the belief that someone would have to plug into the hospital token ring network, or the clinical system itself to even get to it, let alone know how to attack it!

Today a full medical record sells for between $20 and $50 based upon the age of the patient. An older patient record fetches more, probably because that patient has a long established credit rating and has more than likely paid off their mortgage. Ripe pickings then for identity thieves intent on taking out loans on behalf of their victims and siphoning off retirement funds!

"All of the evidence suggests that a healthcare record is in fact much, much more valuable than a financial record. It can be used for financial ID theft crimes, or a medical ID theft or both. It provides a dossier of personal information so bad guys can do more and better stuff like create passports, and visas, and because they have physical characteristics as well as information, it's a big deal. And I see in a number of our studies that it is substantially more valuable than other types of records." Larry Ponemon

And the threat is not just from outside. At one reputable hospital a nurse was found accessing the medical records and patient identities of many of the elderly wealthy patients in her care. After an investigation it was found that she was passing these identities to her cousin in San Diego who purchased new expensive cars in their names and on their credit, then drove them over the border into Mexico where they were sold for cash with a cut in the illicit profits coming back to the nurse. If you can't trust your own people who can you trust to help you?

About CSC

The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."

About the Author

Richard Staynings is CSC's Global Coordinator of Cybersecurity services across the Healthcare industry. He is former Cybersecurity and Risk Officer, a 20 year veteran of cybersecurity and self proclaimed evangelist of secure and safe healthcare services.

He can be reached by email at CybersecurityConsulting@csc.com

For a complete listing of CSC Cybersecurity services go to http://www.csc.com/cybersecurity

For a complete listing of CSC Healthcare services go to http://www.csc.com/healthcare

What can healthcare do to mount a defense before its too late?

'You don't know what you don't know', (which means you don't know what your true risks are) and unfortunately the magnitude and complexity of the cyber threats facing healthcare today are beyond the abilities of many, if not most, healthcare providers, payers and life sciences organizations to detect and defend themselves against.

Knowing what you are up against is the first step to mounting any formidable defense and knowing your strengths and weaknesses is the second step. Most healthcare organizations have been lulled into a false sense of security by a combination of weak non-prescriptive security rules governing the industry, which are open to wide interpretation by the reader, and internal assessments conducted against those weak rules by assessors who are not security professionals and therefore can not fully understand the breadth or depth of cybersecurity risks that need to be addressed.

If you didn't realize it, the entire paradigm of secure healthcare has forever changed. The threats to the industry are now greater than ever before and are expected to continue to rise at an exponential rate as criminals look to the industry and its bountiful supply of poorly protected information as the next great cash cow!

The compliance and regulatory rules have changed as well. HHS Office of Civil Rights (OCR) is on a mission to change the security and privacy practices of the industry and OCR is no longer restricting its investigations to those who are unfortunate to suffer a breach. Nineteen out of twenty randomly selected covered entities failed the new OCR audit rules in 2012. These were not small cottage hospitals with minimal security either. Many of these were leading and highly reputable institutions with large security staffs and comprehensive security controls. If many of the best in the industry cannot pass an OCR audit, there is little hope for the average covered entity or business associate.

With hackers on one side and the OCR with its steep fines and penalties on the other, it's no wonder that many Healthcare CIOs and CISOs cannot sleep soundly in their beds at night.

Covered entities should commission an immediate assessment of their capabilities and controls against not just the HIPAA Security Rule and the Omnibus HITECH Rule, but also against the 77 Point OCR Audit Rule and industry leading security practices based upon ISO 27799:2008 (Information Security Management in Health using ISO 27002), NIST or other cross industry security standards.

To be effective, this assessment should be conducted not by hospital IT or risk staff, but by external cybersecurity professionals who are able to provide an objective risk-based assessment against current known cyber threats, to ensure that all risks are documented in a strategic and tactical cybersecurity roadmap towards compliance. Covered entities will then need to prioritize identified weaknesses with remediation projects to put in place improved security controls before breaches and fines eat into organizational finances. The cost of compliance and effective security is after all, a mere fraction of the potential cost of loss!