Alexander Cannell

11/05/2013

Professor Dempsey

Cyber Security

    A survey given by The Bureau of Labor Statistics in 2012 stated, “On average, the average adult spends 8.0 hours a day on a computer.” (BLS, 2013) I spend at least 12 hours on a computer each day with my job and school work.  But I have a pretty good excuse with the hours that I spend within the “virtual world” because I am a Computer Forensics Major. Our lives are so intertwined with computers, I can’t remember a time when my family didn’t have a personal computer in our household. We can just look at social media today and see how much of our lives are online. Frankly it is quite scary to think that “11% of social network users have posted content they wished they hadn’t. Men [are] more likely than women to post comments they regret…” (ReadWrite, 2012) Not only are we online, but our entire country’s infrastructure is run by computers. Computers play a central role in electricity, oil distribution, water, natural gas, water treatment facilities, finances traffic control.  Almost everything in our lives are controlled by some type of computer system. But what should the role of the Government be with regards to Cyber Security?

    Jonathan Swift once stated, "When a true genius appears in this world you may know him by this sign that the dunces are all in confederacy against him." (Swift, 2012)  Humans in general have been and always will be fascinated and terrified of the unknown. Change is the necessary ingredient for all advancement, and yet change is something very few can accept without a fight. In the quest to understand the world around us and outer space, the Greek Mathematician Pythagoras was the first to propose that the world was a sphere rotating on it’s own axis. This revolutionary idea  seemed absurd to a sixth century BC society that believed in a flat stationary world with dangerous serpents sitting beyond the horizon.  Pythagoras became a social  outcast while the learned of the day insisted that a invisible man in a chariot with flying horses dragged the sun across the sky each day.  Supported by the newly formed Roman Catholic Church, this earth centered universe model remained generally accepted for fifteen centuries. (Carl, 2005)  In that time many scientist like Pythagoras theorized that the current theory was incorrect but few dared to share their findings and those who did were punished for their heretic views. The last of these so called “rebels” was Galileo.  He was  the first astronomer ever to use a telescope, and the last to be persecuted by the church for suggesting that the earth traveled around the sun. He was summoned to answer on charges of heresy. At his trial before the church, Galileo was forced to curse his theory about how the earth moved around the sun. If Galileo had not done this he would have been burned alive at the stake.  Although Galileo complied, he was ordered to spend the rest of his life under house arrest and was allowed no visitors or outside contact with anyone. Immediately after being sentenced a stunned Galileo calmly declared, “And yet the earth moves.” (Peter, 2005)

    In the world of Computer Security we have three different types of hackers, first we have the “White Hat Hacker”, second we have the “Black Hat Hacker”, and lastly we have the “Grey Hat Hacker”. White Hats are people who are under a contract with a corporation or government to hack into  a network.  Essentially,  it is someone with permission to be in the network/computer.   Black Hats are people who have malicious intent in trying or actually gaining access to a network/computer. Now the grey hats are an interesting group they hack networks without permission not for malicious intent, but for curiosity sake. Grey hats are like Batman, the vigilantes of the Cyber world.

    Hack doesn’t just mean to gain access, but to make work in your own way. The term of Hacking didn’t have anything to do with computers, but with Model Trains. In 1946 M.I.T. (Massachusetts Institute of Technology) started Tech Model Railroad Club. M.I.T. model train club (which is still in existence today).  They would use the term “hacker” and apply the term to “someone who applies ingenuity to create a clever result, called a ‘hack’.” (Train, 2013) Now one of the first ever computer hacks was attempted on telephones.  In 1969 Quaker, the cereal company would include a whistle in each box of Captain Crunch.   These Captain Crunch whistles would produce a 2600 herz tone, which could be used to fool the phone company and give the person the ability  to make free long distance phone calls. Understanding how the phone system worked, you could obtain the area codes which were used to make calls to different states, countries, offshore sea vessels, and even newly developed satellites. The Captain Crunch whistle was a great example of Phreaking. (Whistle, 2008)

I believe the greatest hack I have read about would be Stuxnet. In June of 2010 a computer virus was found hiding in the systems of traffic control, power plants, and factories all around the world.  This computer virus was called Stuxnet. Twenty times more complex than any other virus code, Stuxnet had a collection of capabilities among them was the ability to turn up the pressure of a nuclear reactor, or switch off oil pipelines. The scariest thing was Stuxnet could tell the system operators that everything was normal. Unlike most viruses Stuxnet didn’t carry the usual forged security clearances that other viruses do. These forged security clearances  of prior viruses help other viruses burrow into targeted systems. But Stuxnet actually had  real clearance, stolen from Realtek one of the most well-known and respected computer companies in the world. Stuxnet exploited what is called Zero Days which is an unknown vulnerability in a computer system that system creators are unaware of and the most successful viruses exploit Zero Days. Zero Day’s details can be sold on the black market for over a hundred thousand dollars. Stuxnet utilized an advantage of twenty Zero Days. Once Stuxnet got into a computer system it didn’t always activate buried deep within the programming ,  it could live within the system for a long period of time.  The Stuxnet code had a specific target that it would attack.  Without that target, the virus could remain dormant inside the computer system, kind of like a Trojan Virus. A Trojan Virus is a virus that remains un-operational until something or someone activates the virus. Stuxnet was looking to shut down the centrifuges that spin nuclear material at Iran’s enrichment facilities. Stuxnet was a weapon, the first known to entirely be made out of code the Institute for Science and International Security (ISIS) reported that the virus Stuxnet shutdown 1000 centrifuges at the main enrichment facility in 2010 at Natanz, Iran. (ISIS, 2010) In November of 2010 the UN’s (United Nations) International Atomic Energy Agency reported that Iran had suspended work at it’s nuclear facilities without saying why.  (IAEA, 2010) In June of 2011 the Iranian government conceded that the virus infection of the Bushehr Nuclear Facility (which was still under construction at the time) switching the plant on could lead to a national blackout. (Bushehr, 2013) Iran in response to the attack on their nuclear facilities hired hackers to join the Iranian Revolutionary Guard. There is just rumors of who designed Stuxnet. The important question isn’t who designed Stuxnet, but who will redesign it? Stuxnet is available online for anyone to download and tinker with. Stuxnet is the first ever open source weapon. (Missing Link, 2013) (Stuxnet, 2013)

Hacking in the simplest terms is the expanding of the boundaries, exploring the limits, instead of exploring the globe or exploring space as a hacker you are exploring the inner space of telecommunications networks of personal computers and trying to figure out what more you can do. Hacking is an expression of the human drive to know more, to go further to experiment, which is fundamental to society. I think the wild west is a great analogy for hacking. The wild west was a place where laws are never really considered or enforced. Where new things were happening leading to exciting  revolutionary things. Where right and wrong lives in a fuzzy grey area. Grey Hat Hackers like cowboys are individualist of the first degree; they are out there on the edge of the wild west of the outlaw world going out trying new stuff and seeing where the borders are seeing where the monsters dwell. What monsters are out there?

Cyber Crime is any crime that consist of the use of a computer and a network. Cyber Crime ranges from child porn which is the explicit use of children to Internet fraud which is the use of the internet to con people or governments out of money.  We see Cyber Crime continually becoming a bigger problem. Cyber Terror is a kind of warfare on the virtual frontier or viral wild west consisting of either the destruction, or disruption of digital property. Sometimes though, Cyber Terror can leap outside of the virtual realm and into the physical world. For example, automated controls on power systems are attacked and they cause power outages, or they cause dams to burst, pipeline scrubbers may cause a backup in the line eventually causing an explosion, or pipelines to cease their flows.

There is an increasing connection between the virtual and the physical world; unfortunately, this is the realm of the cyber terrorist. Terrorism is the use of violence and/or the threat of violence to produce fear.  Cyber terrorist main  goal is political, and has a reachl of mass media coverage. A terrorist is a radical person that carries or plots to carry out acts of terrorism. A cyber terrorist is someone who uses systems to cause terror. Terrorist groups are looking at the possibilities of cyber terror, but terrorist have to make a decision about whether to develop their own cyber terror capabilities or to recruit others from the outside. On average terrorist organizations don’t like to hire outside help for the security risk, but opt to choose someone within and train someone who is already a radical.

In all this mess what is the role of the government with regards to hacking and cyber security? More specifically what is the role of Homeland Security in cyber security? Should the government go after these Grey Hats?

The cyber world is a scary world, full of people wanting what we have as a free society. It is the responsibility  of the United States Government to protect us from the evil Black Hat Hackers. If our government is unable to protect us from these cyber bullies then we are not going to be free of these villains of the Cyber world. Unfortunately, we don’t live in an ideal world where every criminal will be punished for their cyber crimes.  We live in a world where technology is constantly changing around us, and we have out-dated laws that fail to coincide with the advancement of technology.  In a lot of cases criminals are slipping through the loopholes in our outdated laws. Just look at the case in the United Kingdom where a teenager after getting fired from his job sent five million emails to his ex-employer causing a denial of service attack (DoS attack).  This attack crashed his former employers mail servers. The shutdown of his servers would have meant a loss in revenue, but the case was dismissed because denial of service attacks were not covered under the United Kingdoms Computer Misuse Act (CMA) of 1990.

On the other hand, we have some organizations like the Anonymous group who are supported by the majority of the citizens but technically are committing crimes.  They are considered between Grey Hats and Black Hat Hackers.

The Department of Homeland Security (DHS) as we know was formed after 9-11, in response to that awful terrorist attack of the destruction of the twin towers in New York City. The Department of Homeland Security has three basic responsibilities. First, prevention; Second, response; and Third, recovery. Not so much in field response, but the Department of Homeland Security isn’t meant to have an operational arm. Maybe not having much in the operational is a good thing, or maybe it’s not. Going off the three basic responsibilities we have two major departments within the Department of Homeland Security that handle or combat Cyber Crime.  First, the Secret Services Electronic Crimes Task Forces (ECTFs);   Second, Immigration and Customs Enforcements (ICE)  and Cyber Crime Center (C3). (DHS, 2013)

The Secret Services Electronic Crimes Task Forces, was a mandate in the USA Patriot Act of October 2001.  I states that the U.S. Secret Service is responsible  to establish a federal cyber crime task force. The Secret Service was a part of the U.S. Department of the Treasury before they became a part of the Department of Homeland Security, and even before the Secret Service was a part of the president’s protective detail. So, Naturally the  Electronic Crime Task Force(ECTF) would be given the task to investigating, and preventing “cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes.” (DHS, 2013) What I found interesting is that the National Computer Forensics Institute is run by the Secret Service.

Immigration and Customs Enforcements (ICE) Cyber Crime Center (C3), consists of four cyber investigative services sections Cyber Crime Section (CCS), Child Exploitation Section (CES), Digital Forensic Section (DFS), and Information Technology and Administrative Section (ITAS).  Cyber Crime Center is responsible for Identity and benefit document fraud, money laundering, Financial fraud, Commercial fraud, Counter –proliferation investigation, narcotics trafficking, illegal exports, and their major focus is child exploitation investigations.  My dream job would be to work for ICE and the C3.  (ICE, 2013)

Special Agent for the FBI Frank Harrell stated, “Most hackers are of a non-destructive intent [Grey Hats]. The FBI [Federal Bureau of Investigation] doesn’t track the average White hat hacker; we don’t have the resources, the time, or the interest of doing that. We are specifically motivated in catching the individuals that are breaking federal law…” (Wanted, 2010) I agree with Special Agent Harrell, we need those types of Grey Hat Hackers; the Butch Cassidy’s or Batman’s of the cyber world who are going out there and trying to shut these Black Hat Hackers down. In our justice system it is very hard to make the distinction between legal and illegal when you are talking hacking because intent is very much a part of our criminal justice system we have to realize that in our justice system it is very hard to know what someone’s intent is. I think that you can’t use old models/rules and apply them to these new situation they don’t relate very well. Socrates was sentenced to death by drinking a poisonous herb called hemlock because essentially he wouldn’t recognize the Greek gods, for undermining the customs of the time, and for not committing to the traditions of the fathers. After drinking the hemlock which causes a slow and painful death Socrates stated, "To fear death, my friends, is only to think ourselves wise, without being wise: for it is to think that we know what we do not know. For anything that men can tell, death may be the greatest good that can happen to them: but they fear it as if they knew quite well that it was the greatest of evils. And what is this but that shameful ignorance of thinking that we know what we do not know?”  We as human beings fear change, and fight so hard against even the slightest change, but what if as Socrates stated change is good? Once you start punishing these Grey Hats for pointing out system flaws, less will be willing to come out and identify these flaws.

CITED WORKS –

·        [American Time Use Survey Summary. (2013, June 20). *U.S. Bureau of Labor Statistics*. Retrieved November 8, 2013, from http://www.bls.gov/news.release/atus.nr0.h](http://www.bibme.org/)

·        [[STUDY] Facebook Defriending is on the Rise. (2012, February 24). *ReadWrite*. Retrieved November 8, 2013, from http://readwrite.com/2012/02/24/study\_face](http://www.bibme.org/)

·         Swift, J. (n.d.). Jonathan Swift. *BrainyQuote*. Retrieved November 8, 2013, from http://www.brainyquote.com/quotes/quotes/j/jonathansw132411.html

·         Carl, H. H. (2005, February 23). Pythagoras. *Stanford University*. Retrieved November 8, 2013, from http://plato.stanford.edu/entries/pythagoras/

·        [Peter, M. M. (2005, March 4). Galileo Galilei. *Stanford University*. Retrieved November 8, 2013, from http://plato.stanford.edu/entries/galileo/](http://www.bibme.org/)

·        [TMRC - Hackers. (n.d.). *TMRC - Hackers*. Retrieved November 8, 2013, from http://tmrc.mit.edu/hackers-ref.html](http://www.bibme.org/)

·        [Kovalchik, K. (2008, August 30). TRUE CRIME: John Draper, the original whistle blower.. *Mental Floss*. Retrieved November 8, 2013, from http://mentalfloss.com/article/19484/true-crime-john-draper-original-whistle-blower](http://www.bibme.org/)

·        [Institute for Science and International Security › ISIS Reports › Iran › Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report. (2010, December 22). *Institute for Science and International Security › ISIS Reports › Iran › Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*. Retrieved November 8, 2013, from http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/](http://www.bibme.org/)

·        [General, D. (2011, November 8). Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran. *Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran*. Retrieved November 8, 2013, from http://www.iaea.org/Publications/Documents/Board/2011/gov2011-65.pdf](http://www.bibme.org/)

·        [IRAN (Persia) NEWS. (n.d.). *IRAN (Persia) NEWS*. Retrieved November 8, 2013, from http://cj.myfreeforum.org/archive/iran-persia-news\_\_o\_t\_\_t\_597.html](http://www.bibme.org/)

·        [Kushner, D. (2013, February 26). The Real Story of Stuxnet. *- IEEE Spectrum*. Retrieved November 8, 2013, from http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet](http://www.bibme.org/)

·        [Homeland Security. (n.d.). *Combat Cyber Crime*. Retrieved November 8, 2013, from http://www.dhs.gov/combat-cyber-crime](http://www.bibme.org/)

·        [Cyber Crimes Center. (n.d.). *Cyber Crimes Center*. Retrieved November 8, 2013, from http://www.ice.gov/cyber-crimes/](http://www.bibme.org/)

·        [THE Sprawl. (2010, May 20). *hackers wanted*. Retrieved November 8, 2013, from http://thesprawl.org/simstim/hackers-wanted/](http://www.bibme.org/)

·        [USDOJ: CRM: Computer Crime & Intellectual Property Section. (n.d.).*USDOJ: CRM: Computer Crime & Intellectual Property Section*. Retrieved November 8, 2013, from http://www.justice.gov/criminal/cybercrime/](http://www.bibme.org/)

·        [CYBER CRIME. (2010, March 17). *FBI*. Retrieved November 8, 2013, from http://www.fbi.gov/about-us/investigate/cyber](http://www.bibme.org/)

·        [Security Response Publications. (2012, January 5). *Internet Security Threat Report*. Retrieved November 8, 2013, from http://www.symantec.com/security\_response](http://www.bibme.org/)

·        Nemeth, C. P. (2010). *Homeland security: An introduction to principles and practice*. Boca Raton, FL: CRC Press.

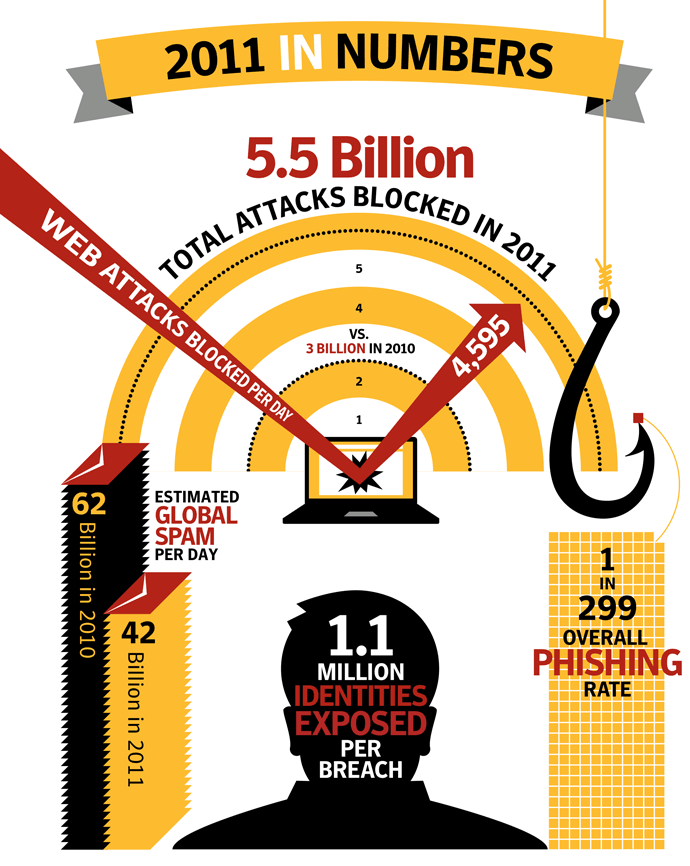


Figure 1: <http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=benefits_in_the_cloud>

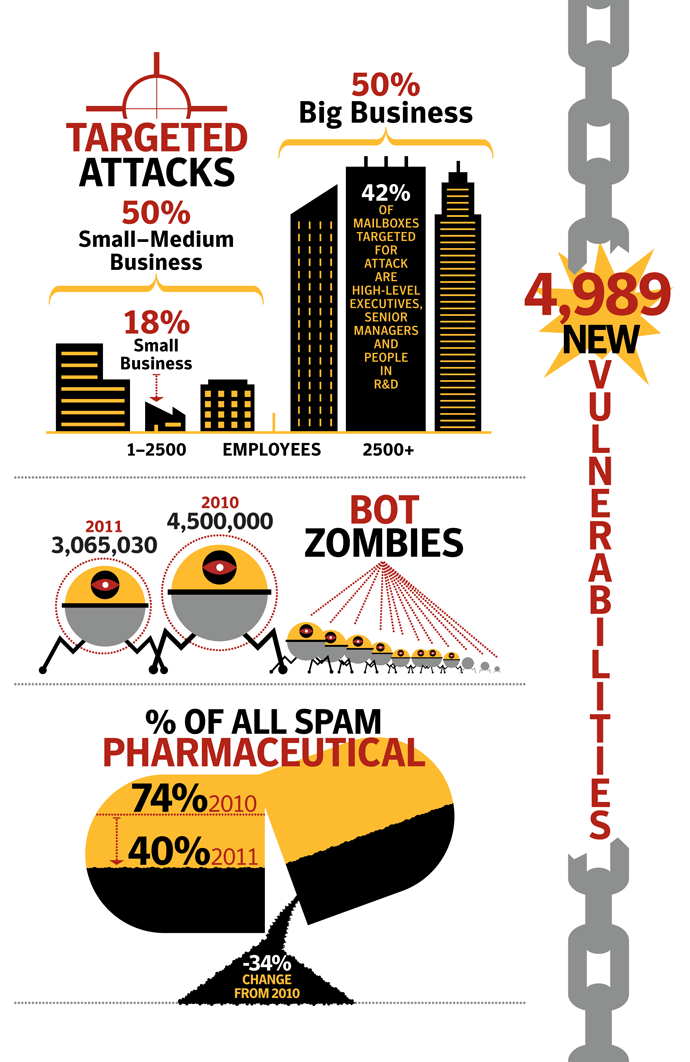


Figure 2: <http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=benefits_in_the_cloud>

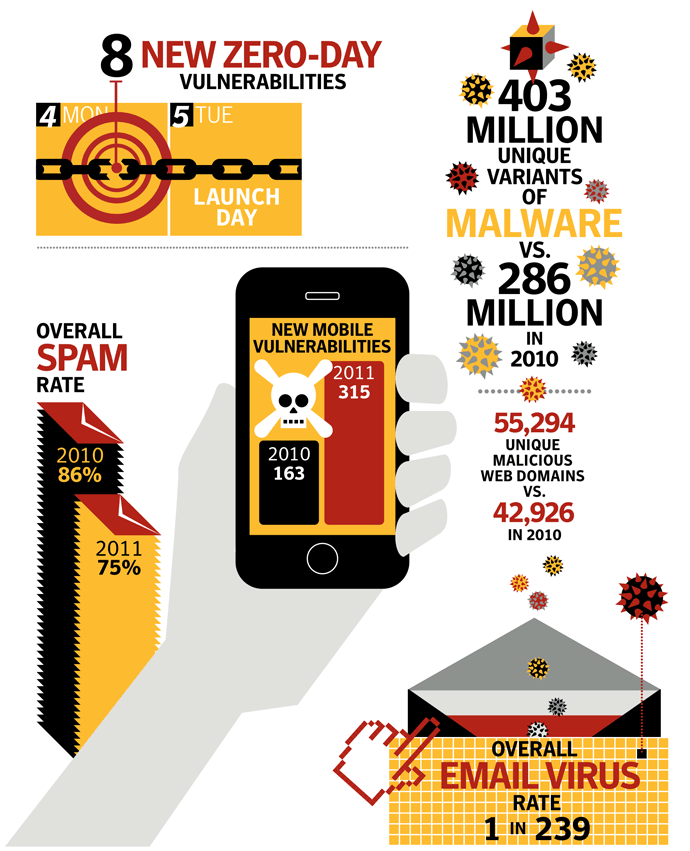


Figure 3: <http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=benefits_in_the_cloud>

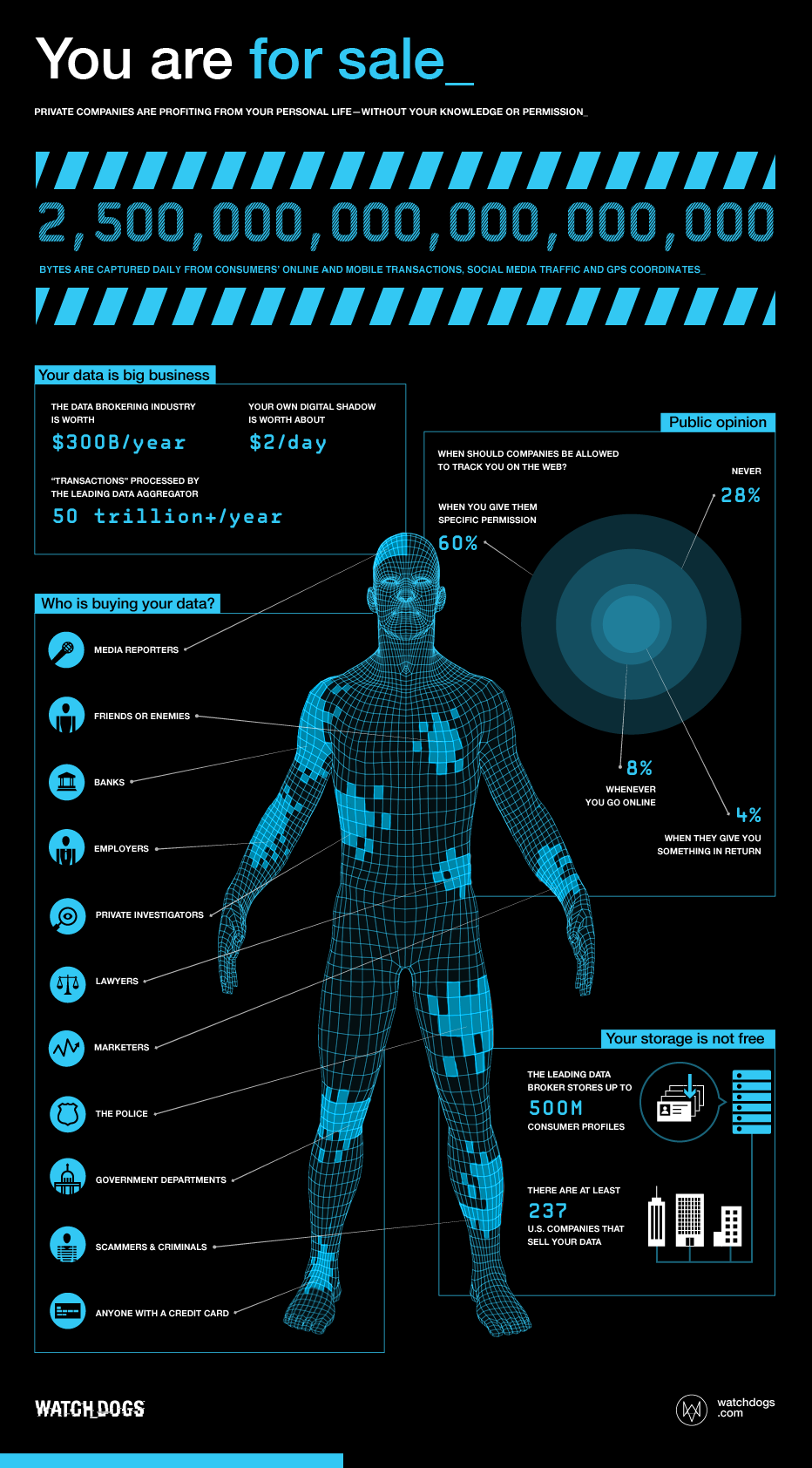


Figure 4: <http://i.imgur.com/yRAolRB.png>

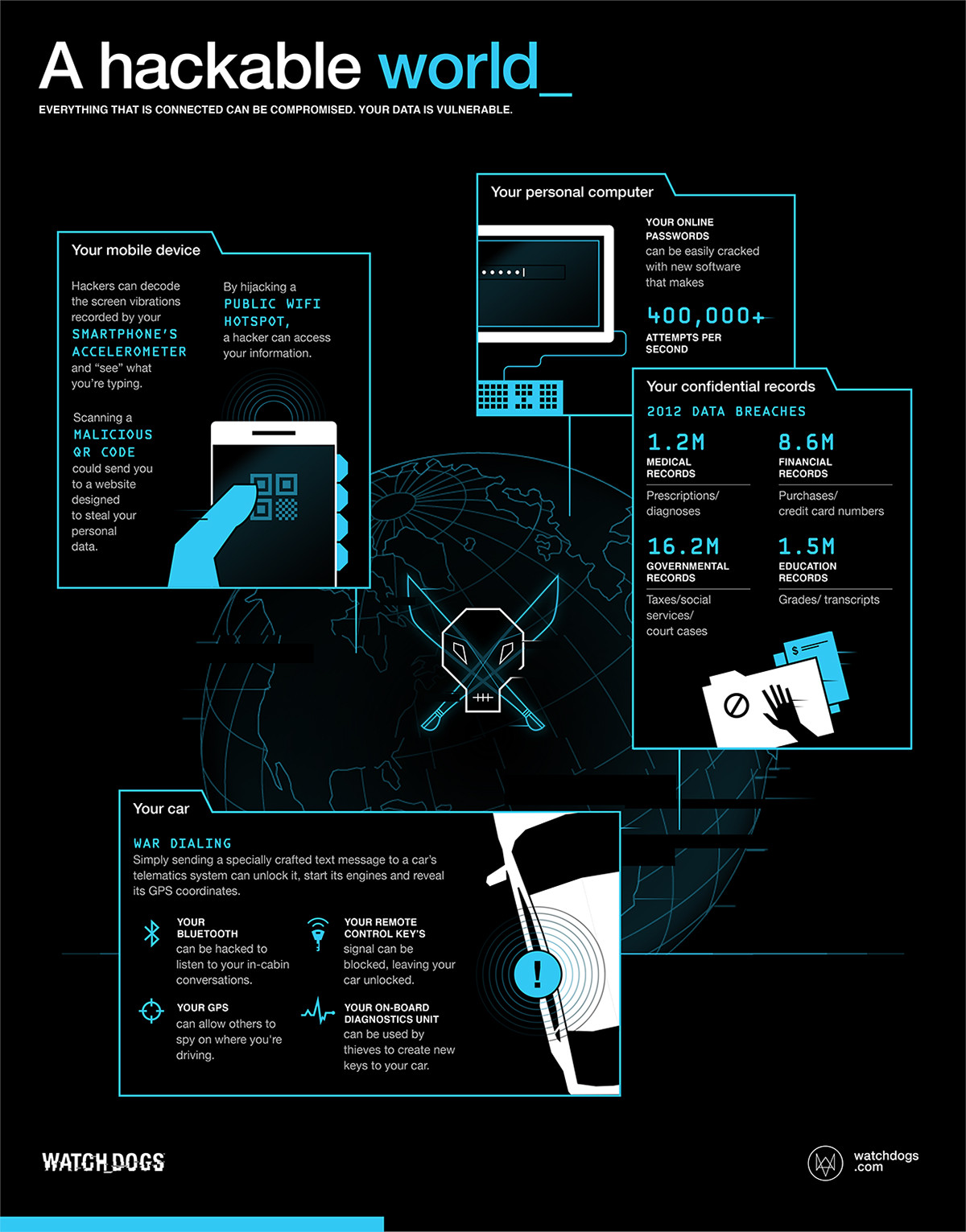


Figure 5: <http://i.imgur.com/nT8TDv9.jpg>