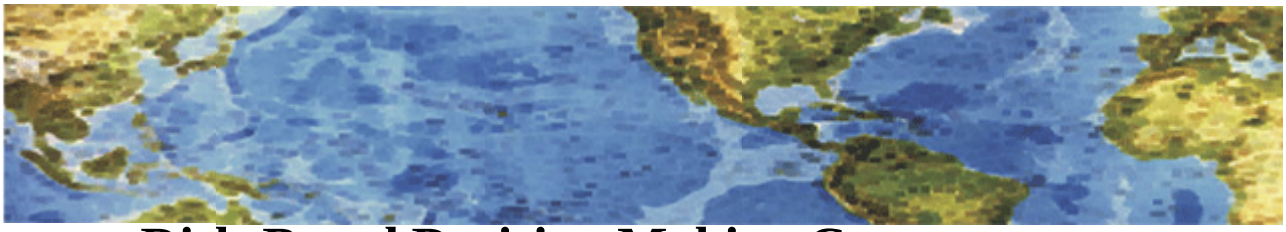
HALL ASSOCIATES



Risk-Based Decision Making Commentary
30 July 2014 Newsletter

8 Cyber-Crimes Expected to Exponentially Increase in Next 20 Years

Many people believe that a number of "traditional" crimes as we know them today will be largely replaced by cyber-crime in the next 20 years. In many cases (see below) this is already happening. Since we are rapidly connecting all of our lives to the world, we are opening ourselves to criminals outside of our personal spaces, buildings, cities. This is already changing how crimes are committed as well as increasing the overall number.

Take bank robberies: According to the American Bankers Association, bank robberies are being steadily replaced by ATM-skimming and other 'cyber-heists.' FBI statistics show bank robberies are down 60% since their peak in 1991, and they plummeted another 23% just between 2011 and 2012. Other crimes are also following suit. Car thieves around the country are now using 'mysterious gadgets' to remotely unlock car doors without having to jimmy the lock or smash the window. Burglars have been robbing hotel rooms using a keyless door hacking tool that was first revealed at the Black Hat hacking conference.

It's time for people to stop thinking of cyber-crime as something that only happens on a computer. With the rise of 'smart' devices and the Internet of Things (IoT), the maturation of the online black market as a multi-billion dollar industry and the widespread commercial and recreational markets for do-it-yourself hacking tools, cyber attacks will become far more invasive, dangerous and even physical.

Here are eight future cyber crimes that could affect you in the not-so-distant future:

1. Cyber-Jacking aircraft. Why bother physically hijacking a plane, when you can simply cyber-jack it? Future attacks probably will leverage some type of cyber attack on the aircraft or its ground support systems. This could range from exploiting the plane's flight management system (as demonstrated by researcher Hugo Teso last year), to attacking ground-based systems that the plane relies on, spoofing or interfering with air traffic control transmissions or infecting the air traffic control system with fake "ghost" planes and making real planes disappear (as discovered by researcher Brad 'Renderman' Haines in 2012).

2. Human Malware - There's a good chance that at some point in the near future, humans will be infected with malware. How could this happen? If you rely on a WiFi-enabled medical implant (e.g., pacemaker, cardioverter-defibrillator, insulin pump, etc.), your body could be physically harmed by a cyber attack on that device. Researchers have already demonstrated that it's possible for a determined hacker to break into your implant and hurt or kill you. But down the road, this threat could become even easier to distribute. New research released earlier this year by the University of Liverpool found that it's possible to spread computer viruses via WiFi routers. Infected WiFi routers could pose a serious long-term risk - particularly with implant patients. In the future, a compromised WiFi network (at a hospital or the Starbucks across the street) could be used to spread medical viruses to patients.

3. Cyber Assault - As networked appliances, home automation systems and wearables become more widespread, hackers will have another way to invade your life - and physically harm you. Because all of these rely on basic operating systems or firmware to work properly and are connected to the Internet, they

can be remotely controlled by hackers - as has been demonstrated already by numerous researchers, including a home appliance 'botnet' recently discovered by one security firm. These attacks could include things like raising or lowering the thermostat, shutting off or malfunctioning appliances (like turning off the refrigerator or bypassing the temperature restriction on the water heater), causing wearables to overheat or making augmented reality glasses flicker bright blinding lights in your eyes. In most cases, these wouldn't put a person's life at risk, but they would make you feel unsafe in your own home. Consider this cyber-stalking taken to the next level.

4. Cyber Extortion. With so much of our personal lives, work and finances tied up in online accounts, anyone who's able to take over those accounts is in a great position to demand a ransom payment. "Ransomware" attacks are already taking place throughout Europe in the U.S. with the so-called 'CryptoLocker' virus and multiple variants. Expect these attacks to become as widespread as email spam in the next few years. However these attacks could become considerably more dangerous, potentially including home, car and smart grid meter jacking attacks followed by payment demands to make them stop.

5. Car Sploiting. Viruses are likely to become a more serious problem for our cars in the near future. As cars become more computerized, their systems (which also include OnStar-type connections and numerous subsystems/computers with Windows, Android, iOS and BlackBerry operating systems) are more vulnerable to attacks, and automotive viruses and malware are likely to spread. Earlier this year, a Formula One racing team had to cut its preseason test short after the vehicle became infected with malware. Ford is taking the threat so seriously that it's already begun testing its car systems against possible hacks.

6. Brick Attacks. When it comes to bank fraud, account takeovers and stolen credit card numbers aren't the only thing you'll have to worry about. What if your account was completely erased from the bank's records? In the "brick attack," hackers don't just try to steal money or information - they just destroy it. They do so by infecting the computers and servers that store this data with malware that renders them completely useless, unable to be turned on again (i.e., 'bricks'). Saudi Aramco, the world's largest oil company, was already hit with a brick attack in 2012, which destroyed 30,000 computers. And in December 2013, the National Security Agency claimed it had foiled a plot by foreign adversaries to "brick" computers all across the U.S. Now imagine attackers hitting a major retail bank/financial institution (like yours) and targeting customer account information. It could happen in the not so distant future.

7. Identity Theft Squared. You think it's bad now with identity theft? Well, just wait. Right now, biometric security (e.g., fingerprint scanners, retina scans, voice prints, etc.) is limited to a few consumer devices, but once it becomes a key way to authenticate your online accounts, biometric data will become an important commodity to the criminal underground. Genetic data theft is also an increasing risk as more consumers sign up for genetic testing and their data is stored on vulnerable networks.

8. Mini-Power Outages. As more homes transition to 'smart meters,' they could also become vulnerable to new types of criminal tampering. Two key features of today's smart meters that could be taken advantage of by hackers are their ability to wirelessly update the firmware and remotely disconnect users. This could allow attackers to corrupt the smart meters of individual homes, running up bogus charges or causing the electrical system to malfunction, shut down or surge (frying all of your outlets and anything connected to them). They could also allow attackers to disconnect homes at will. (And don't get me started on how easy it is to disrupt a major electrical grid).

As our lives become increasingly dependent on technology, we will become more vulnerable to cyber crime, in ways that may be hard to imagine today. While yesterday's criminals are limited by physical proximity, skill and daring, today's and tomorrow's criminals won't face any such restrictions. In the next few years, expect to see a new wave of crime that will require greater vigilance to protect against.

http://www.foxbusiness.com/personal-finance/2014/05/14/future-crime-8-cyber-crimes-to-expect-in-next-20-years/