



Unreported Cyber Crime

A great deal of cyber-crime goes unreported, swept under the rug, so to speak. The FBI's Internal Crime Complaint Center tells us that approximately 286,000 cyber-crime incidents were reported in 2016 with a loss estimate of \$1,300,000,000. In itself, that might sound like a lot of criminal activity, but consider that the Department of Justice estimates are that only 1 in 7 are actually reported. If that is correct, then we are talking about 2,000,000 individual incidents. Talk about tip of the iceberg.

So why aren't the rest reported? There are a number of reasons. For example, if the attack was caused by a mistake you made, and you believe no one will find out, would you report it to your boss? Well, if you are the boss, neither will your employees. Most of the time, it turns out, employee error is the root cause of the problem. Not that your employees will send you ransom notes, but simple errors, usually made by untrained employees, cause the vulnerabilities that let the cyber-criminals in the back door. Maybe Joe clicked on a link when he should have known better, or Mary was tricked into sharing files with someone who only had their own nefarious self-interests in mind. Coming forward can have disastrous effects on a career/job and self-preservation is a strong motive. This is unfortunate because without this information, managed IT cyber-security becomes more difficult.

In an early episode of the sitcom *The Big Bang Theory*, Howard Wolowitz, one of the lead characters and an engineer working on NASA's Mars Rover, decided to impress his date by letting her "drive" the Rover using the remote controls he had in his lab. However, before he could turn the controls over to her, Howard drove the unit into a gully, forever lost. Panicking, he and his

scientist buddies ultimately deleted the entire software program and all records of the Rover, covering his tracks and getting away with it. While we suspect that in real life he wouldn't have been so lucky, the incident drew its humor from the fact that people will try and cover their tracks rather than admit to serious errors they have committed. The same will often hold true even if that employee is able to assist in fixing the problem, not wanting to admit to the mistake in the first place.

As the boss, if you believe that going to the trouble of reporting the attack won't lead to anyone's arrest, or the prevention of future crimes against you, would you report it? Statistics say you won't.

And while the crime fighters in DC will tell us that all these crimes should be reported, and that ransomware demands should not be paid, it's usually easier to just pay up and move on...except that about 20% of the time, the encryption key that the business owners paid for either never arrived, or simply doesn't work. Here at DynaSis, we worked with one company that refused to listen to security advice, claiming they were too busy and that they would get to it later on, and therefore was unprepared for

a cyber-attack. They were hit with ransomware, ultimately paid the ransom, but never received a workable encryption key. Two separate forensics companies were brought in, but the files were never recovered. They had previously digitized all their files and destroyed the paper originals...they lost two decades of records.

[\(Read more\)](#)

Another reason for the lack of reporting is that many cyber-crimes are well-hidden, either intentionally by the perpetrators, or because crime fighting techniques are behind the times. The New York Times recently reported on three crime waves that were taking place under the noses of law enforcement because they didn't have, or didn't use effective technological tools:


- > Law enforcement officials in Utah realized that in their fight against the opioid epidemic, their investigation was being impeded because they did not have up-to-date data on the online sale of fentanyl, so they brought in a team of analysts to track these sales and see if they could determine patterns. These online sales are a form of cyber-crime and were previously unreported.
- > Philadelphia detectives were treating each cyber-phone theft and sale as a separate crime but ultimately realized that they were all connected through a sophisticated ring of thieves who shared connections to steal and then sell the phones.
- > A digital age crime ring in Nashville was emailing extortion threats to a large number of men claiming they were going to expose their extra-marital relations. Of course, the extortionists actually had no idea who these men were nor if they were actually engaged in these affairs, but the scheme was rather profitable as a number of these victims forked over bitcoins to protect themselves.

These are cases where law enforcement realized that their tools were outdated and did something about it, but each was a difficult task because they were fighting without the benefit of geographical borders and thus keeping track, as well as tracking them down was difficult. It also illustrates the reality that when people publish stats on reduced crime rates, they often overlook the tremendous increase in cyber-crime. Since these crimes may affect their community, even if they may not have been initiated in their community, leaving them out of the stats is a convenient oversight.

"You have to go back to the 1950s to see crime this low," Bill de Blasio, New York City's mayor, stated recently on "Morning Joe" (MSNBC). He was correct in terms of robberies, murders, rapes, etc., but his numbers failed to take into account the rising number of cyber-crimes, reported and unreported. The NYPD's crime tracking system doesn't take these into account and ignores the fact that there are two things going on at the same time: traditional crimes are trending downwards while a new class of crimes are trending upwards.

While the nation's cities may take comfort in misleading stats like this, the FBI, fortunately, is working to correct this situation, along with progressive police departments across the country. In NYC's defense, we will state that while the mayor's statements may be good politically, the city is working towards improved overall reporting. The problem we see is that unless business executives are made aware of the reality of the situation, they will be less inclined to provide the data law enforcement needs.

While many of the cyber-crimes shown above may not be of the type that might affect your business, understand that a crime is a crime and the techniques that were used in these instances are often the same as those used against businesses. Reporting leads to data and data provides information that managed IT support companies and law enforcement can use in prevention.



When people publish stats on reduced crime rates, they often overlook the tremendous increase in cyber-crime.



In 2016 there were 10,000 cases of tech support fraud reported with a reported loss of \$8,000,000 (\$800 per case) but some law enforcement people believe that this, too, is just the tip of the iceberg...

Tech Support Fraud

We all know better than to give a stranger access to our personal computers, just like we wouldn't give that stranger the key to our front door. Your computer likely ties you to your bank accounts, and any number of other private documents. Your work computer is just as data-rich for the cyber-criminal, maybe more so, which explains why the FBI is reporting a significant upward trend in tech support fraud, both in your home and in your workplace. As a [managed IT support company](#), we take every precaution and work very diligently at keeping your IT network safe. So do most other support companies.

The simple fix is to not give anyone online access to your computer unless you know exactly who they are and, in the workplace, not unless you have received permission to do so from your supervisor. Your managed IT service company will already have the information it needs to access your desktop or laptop units and won't need any additional information from you. If someone calls and claims to be from your [IT support provider](#), they will be able to access your computer and install whatever patches, updates, new software, etc., on their own. If they ask for your login credentials, be suspicious...very suspicious. (At DynaSis, we accomplish most of this work overnight so your work flow won't be interrupted.)

While many IT support fraud cases are perpetrated directly against individuals not companies, this does directly affect

businesses because in today's work environment, many employees have company data on their personal units.

How frequent is this version of cyber-crime? In 2016 there were 10,000 cases reported with a reported loss of \$8,000,000 (\$800 per case) but some law enforcement people believe that this, too, is just the tip of the iceberg and that a multiple of these numbers is more likely. In some cases, people may simply not be aware that their information has been stolen and is being used. For example, if the hacker gained access to your personal or company owned laptop, and then used that information to gain access to your company's IT network and then steal customer records with personal information, or confidential intellectual property information, this breach may go undetected for a very long time, and, consequently go unreported. In the famous [Home Depot data breach](#), the criminals gained access to the company's network through a vulnerability in the IT network of one of their smaller suppliers.

In other cases, perhaps the information did not yield a reward for the perpetrator, so you will never know and never report it. (It's still a crime even if there was no benefit to the hacker.)

In today's world, data is king. Without data, it's hard to compete. This includes data on cyber-crimes of all types, no matter how big, no matter how small, no matter how embarrassing. It is our responsibility to report each and every incident as soon as we are made aware. Without this knowledge, we are tying the hands of those who are working to protect us.