Cooperation Between Industry and Law Enforcement to Fight Cyber Crime

by Shawn Gratton

Abstract:

One of the things we learned in the Fall 2017 Cyber Security class at Tufts is that sometimes not all of the best solutions to a problem are technical. Credit card fraud and other cyber crime, for example, can be resisted by a defense in depth approach with such technologies as point to point encryption to tamper resistant hardware. However one big piece of all this defense is the cooperation, both proactive and reactive, with law enforcement. This includes everything from keeping track of the latest fraud techniques to convincing foreign governments to extradite cyber criminals.

In this paper I will cover some case studies of successful and failed examples of industry teaming up with law enforcement and the strategies and tools that they used. I will also cover general guidelines and best practices, such as information sharing, honey pots and research initiatives. Lastly I will discuss areas that could be improved in the future and how that might be done. Anyone who is interested in learning more about how their organization can help fight against cyber crime or how successful anti-cyber crime initiatives were structures should find this information to be particularly useful.

Introduction :

Today much of the world's commerce takes place across networked computer systems, and so financial criminals have followed it there. This is cyber crime. Put simply, cyber crime is crime done over the internet, as described by the Cambridge Dictionary[1]. More thoroughly, it is exploiting weaknesses in the underlying implementation of networked systems or the people who use those systems for gain, financial or otherwise. Many techniques were developed over the years for dealing with financial crime, such as mandating a debit for every credit and cryptography for ATMs[2].

However, opening up financial systems to large scale public networks like the internet creates many new areas for criminal activity and massively complicates the security aspect of those systems. Although many technical solutions exist, one very important area of security of these systems is not about technologies but about criminology and the law. This includes not only preventing and responding to cyber crime but also things such as national security and international relations, for example stealing money to fund terrorism, and even areas such as privacy.

But more generally, it includes cooperation between industry, with their vast expertise, and with law enforcement and their legal power and responsibilities to the public. This, however, brings us to the next topic: Why would industry and law enforcement cooperate? In this paper I will attempt to answer this question.

To the Community:

I wrote this paper as part of the “Introduction to Cyber Security” course at Tufts university. My reason for writing this is because I wanted to take some time to go over both the consequences of bad security, e.g. having to take part in an investigation or testify in court, and also about ways to have good security which are not 100% technical solutions. Although I believe an overview of law enforcement in the realm of cyber security is a worthwhile paper I also believe that people nowadays tend to be too naive and even timid about doing anything that seems to be a hard manual or intellectual problem like crime fighting, preferring instead simple checklist answers like a “plugin” or an “app”. Certainly even thinking critically about policy is hard for some people.

I hope that providing an illustration of the tools, traditions and reasonings behind the law enforcement side of cyber security and some real world examples of these things in action will pique the reader’s interest and perhaps spark some thoughts or discussions. I want the reader to feel inspired to learn more rather than want to either ignore or pretend they already know everything about the topic.

Overview and Analysis:

Industry, although very large and with a great number of resources, lacks the kind of investigative power of law enforcement. However, it excels in other areas. Industry is capable of maintaining their its standards, such as PCI DSS, and code scanning services like Veracode which can help prevent data breaches by detecting things like SQL injection vulnerabilities. These things can be very valuable, especially when combined with law enforcement, for example presenting a data breach audit as evidence at a trial.

Law enforcement has a duty to protect the people they serve from violations of the law. For example, the United States Federal Bureau of Investigation, FBI, describes using “All lawful investigative techniques and legal tools” to enforce federal laws[3]. From launching string operations to actually go in and arrest criminals to working to prod governments to extradite criminals for prosecution in the countries where the crimes were committed the powers of law enforcement can be great. It also has many professionals at its disposal such as investigators and various subject matter experts.

This is not to say that working with law enforcement is always a positive experience. Legal red tape or fear of overly intrusive police activity may make industry reluctant to work with law enforcement and any mistrust or mad experiences may leave the industry party less enthusiastic to assist in the future. Industry tends to want to be left alone and when working in a legal case any imposition of rules and regulations may irritate them unless it is wholly directed towards another party.

So to put it all together, law enforcement has broad legal powers for investigation as well as a great deal of talented personnel. Industry has a great deal of knowledge about specific areas such as finance and certain types of computer systems. Government agencies and industry can work together on things such as hardware security modules and the FIPS[4] standard or the DOD 5220[5] standard for data wiping. These are good standards but there is also a great deal more potential for actually detecting, investigating and even apprehending the perpetrators of illegal activity. That is where the next section

comes in.

Techniques to stop Cyber Crime:

As mentioned earlier, although there are many technologies which can be used to prevent or at least respond to cyber crime, having a policy of studying and gaining a better understanding of cyber crime is superior to simply ignoring it and depending solely on the tools. However in order to do the studying and know what you are up against there has to be some kind of process for doing so, the same as with other crimes such as cheating at gambling or kidnapping.

Training

One major way this is handled is through training of both law enforcement, industry and researchers on the subject. The same way that people may take courses on driving safety. One law enforcement organization, NW3C, is composed of various US law enforcement agencies and offers courses for law enforcement on areas such as how to request information on users of various online services such as Discord or crimes related to Pokemon Go[6]. They also offer training on financial crime and basic computer skills for law enforcement. Another organization, NCFTA[7] also has courses intended for researchers to learn about cyber crime and related areas such as the TOR network.

General education and awareness can be very useful, such as in the case of teaching software developers about SQL injection and cross site scripting and how to prevent it. However one issue that was surveyed in a 2013 HTCIA report[8] is that some organizations do not have a large budget for cyber crime. However at some point it becomes necessary to bring more to bear against the criminals themselves.

Training also helps to reduce the mistrust problem. One way is for industry to make sure they have best practices, which may sometimes be required by law as in the case of HIPAA[9], for handling security and data breaches or other crime investigation. This could be dedicated security professionals, managers, perhaps even most or all employees, or whoever an organization decides is most appropriate. They could also team up with law enforcement from the start, helping with best practices and how different technologies work. On the law enforcement end, law enforcement agents should get adequate training and be able to provide as much assistance to industry as they can in such events as, for example, a data breach.

Teaming Up

One other thing to mention about mistrust, is that both law enforcement and industry, aside from training mentioned in the last section, should also be able to work directly on the security issues themselves. That is to say that industry, academia and other experts should be responsible and take part in any legal discussion, such as writing a new law, that may otherwise not be written with the best knowledge of the subject at hand. The same with law enforcement as they are the experts of their

domain and perhaps even some academic or industry areas such as forensics. Though it need not be a legal case for this to be a good idea, even an industry standard is worthy of such cooperation.

On September 9th, 2014 the PCI Standards Security Council, a standards organization for the payment card industry, issued a statement on data breaches[10]. One of the things they mentioned is that although they suggest various ways for organizations to guard against data breaches that one key element is support from law enforcement. Industry, even in the case of very large companies, does not have policing powers, nor extradition treaties, which are needed to apprehend suspects and put them through the due process of law.

In the event of a breach, or even before e.g. someone caught trying to install a skimmer on a card machine in a store, industry processionals will need to work with law enforcement from actually contacting them to possibly testifying in court. And the laws themselves can be broad such as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 which provides criminal penalties for unauthorized access and use of a computer[11]. This can be used to prosecute cyber attackers for things such as infecting networks with worms or gaining unauthorized access to corporate email servers.

These laws change over time as the public may become concerned with new vectors of attack or for any number of other reasons. But in general they provide a legal way to prosecute attackers who do things which may not, or at least not easily be, prohibited under previous laws. Ideally knowledge of these laws, such as what evidence you would need to convict someone or how much information you could legally request from an online service with a warrant, should be combined with the previously mentioned training both for law enforcement and for related industry professionals. This way the two parties can maximize their ability to both build appropriate defenses as well as to launch an crime investigation when needed and without delay.

Research

Research itself can be done on crime data, such as compiling statistics on different types of attacks or attack vectors and how they change over time. Working with researchers and law enforcement to compile these lists is part of the process. This can then be used to both go back train industry and law enforcement as well as to try and predict what areas new crime may occur in and put up a good defense in that area.

Research cannot always be speculative though. The only real way to learn more about what techniques criminals are actually using and how defenses do and do not work against them in the real work is to study real crime in the wild. One great technique for building up samples, everything from the latest malware to intrusion attempts, is the honeypot technique, explained below.

Honeypotting

A honey pot is basically some type of program, usually a server e.g. a database or web server, which monitors attempts to access and perform actions on it without authorization[12]. These attacks can be compiled and analyzed for use in defending against them in the future. Specialized honeypot software exists, Kippo for example, although a honeypot could be something as simple as letting an attack into a real network and observing them if they are not causing much damage, a small denial of service attack for example.

Not only can honeypots be used to build up a network of knowledge about real attacks, but they can also be used to help catch criminals when used with law enforcement or some type of internal security, though this is a very large and complex topic by itself.

Case studies:

Have you ever wondered what happens when a data breach is discovered or how cyber criminals are actually found out and apprehended? With that understanding of the strengths of law enforcement and industry as well as the power of research we can now delve into those things by looking at real examples of how cyber crime is actually combated.

Skimmers

One area where law enforcement has acted as a deterrent as well as provided assistance and collaboration with industry has been combating credit card skimmers. A skimmer is a device which can read and then store data from a credit card when the card is used. This can either a magnetic track or, for EMV cards,data from the chip or a pin associated with the card[13]. This card data can then be either used to make fraudulent transactions or sold on the black market. It can be done by either outsiders gaining access to the card readers in a store or as an inside job by employees of the store.

Although skimmer fraud was much reduced in Europe compared to the United States due to EMV cards not being in use in the states, such attacks are not reduced entirely and there are other vectors as well such as malware on a smart phone stealing card numbers when entered and sending them to a server. And of course, as in this case, just because a technique exists which can reduce the amount of negative occurrences that happen, chip and pin cards in this case, that does not mean everyone will actually use it.

The massive amount of effort being exerted to try and stop skimming and similar types of credit card fraud is based on two different areas: Education on techniques for stopping the fraud and investigation of the fraud itself. Investigation includes both learning more about how fraud works as well as actually arresting the people installing or attempting to install the scanners. The research from this can then go towards educating merchants, consumers and others about how better protect themselves.

This would not be possible without all of the assistance from law enforcement who actually go out and apprehend the, frequently as part of organized gangs, individual perpetrators. People with the skills to actually perform these attacks on payment systems may be less inclined to when faced with the threat of component law enforcement and an industry that works closely with them[14].

One example mentioned by Hayes is the “Lebanese Loop” where authorities discovered a card trapping technique used by thieves to steal the actual cards. Knowledge of this type of attack and how to prevent it goes from law enforcement into industry. Another good example is the case from 2014 where a professional card thief, Roman Seleznev, was arrested in the Maldives where he was found with 1.7 million stolen credit card numbers[15]. Cracking down on this type of activity, and the research data found during investigations like this are helpful in combating credit card fraud and is a complement to developing new preventative measures.

Sting Operations

Moving on from arresting people after crimes were committed, we now go to the realm of sting operations. A sting operation is when law enforcement try to infiltrate some kind of criminal enterprise and then arrest the perpetrators in the act. One reason that makes it fascinating in cyber security is that, as long as they can happen at any time, it may cause fear and mistrust in criminals and give them pause before getting to bold in their endeavors. And because it is a cyber crime they will also be connected, in some way, to the victim or to an accomplice who may very well turn out to be a law enforcement official.

One great example of this is the activity by the French DST, “Direction de la Surveillance du Territoire”, in 1990[16]. In this case the DST was able to arrest hackers who had been invited to a fictional CCCF (Chaos Computer Club France) hacker meeting, in fact run by the DST. This helped to prevent French hackers from organizing themselves during the early 1990s.

An even more successful example was the “web snare” in which 100 suspects were arrested and convicted in cases involving over 200 million dollars in stolen money by the FBI’s Cyber Division[17]. This is an example of not only of successful law enforcement activity in the cyber realm but also an example of industry getting a great deal of help from law enforcement an increasingly important area. As long as large scale operations like this continue it will be much less profitable to be a would be cyber criminal.

Honeypots in Sting Operations

Honeypots, as mentioned previously, are great tools both for collecting research and possibly even tracking attackers. They go beyond just tools because they are not just tools themselves but part of a strategy to mislead, trap and observe malicious behavior. They can be tested by industry and academics, or by law enforcement agents themselves and used as often as is practice. Once becomes standard practice more and more research is built up and makes it easier to stop this malicious activity. Though doing so too much may bring its own problems but that is a whole different topic.

One example of a honeypot in action which can be used both to find people who were trying to do something illegal as well as, even without actual arrests, convince people that online anonymity is not as strong as it seems, is “Operation PIN” done by various Anglophone countries[18]. The gist of it is that the police would add websites with links promising explicit content which would in fact give messages when clicked that the police have been alerted. Arrests can be made this way but even if they are not it still creates unease and reluctance to take part in such activity.

The last thing to talk about is extradition. I mentioned this already in a previous example but I would like to go into the reasoning behind it. The idea is that, since you are connected to the worldwide internet, you can commit a cyber crime with the victim in another part of the world and your local law enforcement will not attempt to prosecute you. This falls apart if countries start making treaties or at least small deals send the actor to the nation where the crime actually occurred for prosecution. This is not really a technical solution at all but a means to reduce the protective service of the attackers. An it involves law enforcement but also industry in that they pressure their governments to get these treaties in the first place.

Lessons:

The main lesson that I want to give in this paper is that there is much more to good policy, especially cyber security policy, than blinding using tools and checking off lists. There is the whole tradition of law enforcement investigation along with the rule of law and the tradition of research and investigation by both academia and industry which can be used as the body of a good policy. Security professionals should be knowledgeable and proactive about threats and methods of defense, their responsibilities under the law and how they can continue to do better just as cyber criminals will try to get more clever and more powerful.

For someone working in industry, be it payments, software or anything related to the cyber world in general, you should be mindful of this. It may not change what you do at all times during your job but you should at least think about things such as how what you are doing effects security and how policy or even laws could be better to help maintain the security triad of Confidentiality, Integrity and Availability. Is something too restrictive or maybe not restrictive enough? Just like stepping back to look at the big picture of what your program does, looking at technical and non technical details of security is something you should be able to do.

Summary:

In this paper I touched on the relationship between law enforcement and industry, strategies that they use to combat cyber crime and some examples of those strategies at work. This includes research and development with industry help and sting operations using law enforcement’s legal powers. Law enforcement and industry in the broadest sense need to be very proactive and touch on many areas when reasonable to help improve cyber security. Much of this includes diving into the issues and the gritty details of the technologies themselves. This way the two great players in cyber security can both use their strengths and shrink their weaknesses, and rely on their correct actions rather than solely on tools.

References

1 Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/cybercrime

2 Ross Anderson, Security Engineering, Section 1.3

3 FBI, Addressing Threats to the Nation's Cyber Security, https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/viewv

4 NIST, https://www.nist.gov/information-technology-laboratory/fips-general-information

5 archives.gov, https://www.archives.gov/isoo/policy-documents/eo-12829.html

6 NW3C, https://www.nw3c.org/

7 NCFTA, NCFTA Training, https://www.ncfta.net/Home/Training

8 HTCIA report on cyber crime investigation, https://htcia.org/htcia-report-of-cyber-crime-investigation/

9 Department of Health and Human Services, 45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf?language=es

10 PCI-SSC, PCI SSC Statement on Recent Data Breaches https://www.pcisecuritystandards.org/pdfs/140909_PCI_SSC_Statement_on_Recent_Data_Breaches.pd

11 Federation of American Scientists, Federal Laws Relating to Cyber Security, fas.org/sgp/crs/natsec/R42114.pdf

12 SANS Institute, Fundamental Honeypotting, http://www.sans.org/reading_room/whitepapers/detection/fundamental-honeypotting_2054

13 PCI-SSC, Skimming Prevention: Best Practices for Merchants, https://www.pcisecuritystandards.org/pdfs/skimming_prevention_overview_one_sheet.pdf

14 Darren Hayes, Skimming the Surface: Skimmer Fraud Investigations, https://www.researchgate.net/profile/Darren_Hayes2/publication/317036277_Skimming_the_Surface_How_Skimmer_Fraud_Had_Become_A_Global_Epidemic/links/59299d21a6fdcc4443584519/Skimming-the-Surface-How-Skimmer-Fraud-Had-Become-A-Global-Epidemic.pdf?origin=publication_detail

15 Krebs on Security, Carding Kingpin Sentenced Again, https://krebsonsecurity.com/2017/12/carding-kingpin-sentenced-again-yahoo-hacker-pleads-guilty/

16 Phrack magazine, Issue 64, http://phrack.org/issues/64/17.html

17 Jeremy R. Poch, Cyber-Crime and the Uphill Battle Faces by the Business World, http://www.srlaw.org/Current%20Issue/VOLUME%2026%20-%20JULY%20-%202017/Cyber-Crime%20and%20the%20Uphill%20Battle%20faced%20by%20the%20Business%20World.pdf

18 Australian Institute of Criminology, International Police Operations Against Child Pornography,http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi296.pdf