Global Knowledge®

Expert Reference Series of White Papers

Cybercrime 101

1-800-COURSES www.globalknowledge.com

Cybercrime 101

Bob Withers, CISSP, C|EH, C|HFI, E|CSA/LPT, C|EI, Global Knowledge Master Trainer

Introduction

During the 1920s and 1930s in the United States, there was a rather famous bank robber named Willie Sutton. He was called "The Gentleman Bank Robber" because of his demeanor and natty dress style. Ultimately, he was arrested. Recycling an anecdote from an earlier blog, the authorities reportedly asked him why he robbed banks. As the legend goes, he responded, "Because that's where the money is." As far back as six years ago, an episode of “60 Minutes” on cybercrime and cyberwarfare interviewed Shawn Henry of the FBI. Now at CrowdStrike, Mr. Henry talked about a coordinated raid on the banking system in 29 countries through simultaneous withdrawals at ATM kiosks. This crime, which cost ten million dollars, was performed using stolen credit card numbers. (Ref: https://www.youtube.com/watch?v=xUPYblv_8jA&list=PLE9C724FB26259409)To paraphrase Mr. Henry it would be "front-page news" if that was carried out with guns blazing. Hackers, then, are committing cybercrime across the Internet with techniques ranging from identity theft to stealing credit cards to stealing intellectual property in order to profit from their crimes, commit espionage, or for geopolitical and social causes.

Considering the credit card black market and the theft of information from major retailers, hotel chains, and restaurants, the value of the cybercrime grows dramatically.

For the victims—individual or corporate—the consequences are personal. When a criminal accesses someone's personally identifiable information (PII), financial information, identity, or personal health information (PHI) and uses it to carry out fraud, the effects have been likened to the sense of violation and mourning that matches being told they have a serious health problem. After a breach, businesses need to expend resources to close the vulnerabilities that the criminals exploited and (perhaps) compensate customers financially or with services such as Identity Theft Protection. They also suffer the intangible costs (we call this qualitative risk) of loss of customer trust and loyalty. Even if a company isn't charging for services (such as an information website,) the lingering "bad taste" of the cyber-attack stays with the consumers.

Victims of Cybercrime

Broadly, as in life, we can look at the victims of cybercrime in three realms: individual, business, and governmental.

Carried out against individuals, the purpose of the attack may be to gather PHI or financial information to carry out an electronic robbery. Alternately, it may be to commandeer the victim's system into a so-called Botnet and then use the victim computer for sending SPAM or for a Denial-of-Service (DoS) attack. Here, as well, the bad actors may be cyber-gangs, individuals, or nation-states.

Cybercrime against consumers takes on two forms, but the results are generally the same. An individual may have their financial information misused or their "identity” stolen. For example, criminals have stolen my credit card number to rent hotel rooms in Accra (the capital of Ghana) and someone once tried to bail a friend out of jail with my information. Obviously, the latter did not work out well for any of the criminals, either in custody or soon-to-be. A much tougher problem for individuals occurs when "identity theft" takes place and the criminals use someone else's PII to obtain a loan or perform some other action that appears on the victim's credit report.

Individuals can also be victims of personally directed cybercrime. Stories of cyber-stalking, cyber-bullying, and online harassment regularly appear in newspapers and on news websites. With the growth in use of social media, this has taken on a new importance.

Businesses must be concerned about the theft of their customers' information, whether that is account information, residential and email address, or payment data such as credit card information. Hacks that disclose PII and financial information have been in the news continually (it seems) since December 2013. Facing customers and the Internet, website defacement can prove an embarrassment (at the least) to a company, as can having their Internet presences brought down by DoS attacks. Responses to these attacks cost money and resources to fix. They also engender lack of trust amongst their customers.

Organizations have an additional worry: disclosure of sensitive company information such as product plans and engineering specifications. When competitors can take advantage of leaked insider information, they can alter their plans or release schedules to beat their rivals. Whether these breaches come from the inside (such as a disgruntled or subverted employee,) or from the outside (an external hacker,) when this sensitive information is released, the effects on a business can be catastrophic.

Companies must protect their employees' information such as home addresses and telephone numbers, payroll data, and medical records. Aside from the opportunity for identity theft carried out against an organization's workers, this sensitive information can be used for other nefarious purposes.

Governments, lastly, face the same challenges as individuals and businesses. Beyond that, there are the threats from nation-state hackers such as military and diplomatic espionage. So-called "Hacktivists" and hackers who attack for political, religious, or philosophical causes (terrorists who use cyber means) are a threat to civilian and military systems, as well as to critical infrastructure such as communications and power distribution.

Cybercriminals

I tend to group cybercriminals into four groups: individuals, cyber-gangs, so-called hacktivists, and nation-states.

When looking at individual victims of cybercriminals, misdeeds such as cyber-bullying are often carried out by someone the victim knows. While this is not always the case, especially with celebrities, the motivations of the attacks are personal. Twenty-first century crimes such as cyber-stalking, online harassment, and posting personal information or other embarrassing information (such as personal pictures) are often carried out with selfish or self-centered motivation. In the cybersecurity community, this is known as "doxing."

Cyber-gangs often operate in countries and locations where they can act with impunity. Whether from Eastern Europe, Third World countries, or Asia-Pacific, the motivation is usually financial. Looking at http://www.datalossdb.org, for example, many of the top nine largest data breaches occurred in China or the Korean Peninsula. The primary goals are theft of individual financial information through phishing scams or wholesale theft of PII from banks and other businesses. Their range of activities includes creation and maintenance of Botnets, rental of these botnets to other criminal organizations, and the resale of the stolen information.

Hacktivists, as they call themselves, combine hacking and activism to propagate their messages. The main tools in these hackers' toolboxes are DoS and website defacement. It appears that their targets are mostly high-profile corporations and businesses. While hacktivism is still ongoing, it reached its peak during the era of the Anonymous (ed: Anonymous is the name of a group. Cf: the book "We Are Anonymous" by Parmy Olsen) attacks and offshoots such as Lulz Security. Parmy Olsen, a reporter for Forbes Magazine, published an excellent exposé in her book, "We Are Anonymous." Likewise, young Russian hackers were convicted for launching attacks against the Internet services in the country of Estonia.

Lastly, evidence shows that nation-states engage in cyber-attacks across the globe. Whether hackers choose to retaliate for malware such as Stuxnet; or engage in military, diplomatic, and transnational espionage, or theft of businesses' intellectual property, state-sponsored actors often operate with impunity. As an example, in May 2014, the US Department of Justice indicted five officers in the People's Liberation Army (PAL) working for the People’s Republic of China (PRC) for hacking into American companies.

Direct and Indirect Cybercrime

Cybercriminals commit their illegal acts directly against individuals, organizations, or governments through means such as malicious software (malware) or attacks against individual systems. They can also act in indirect manners such as identity theft, financial fraud, or sale of stolen proprietary information.

Direct Cybercrime

While businesses and governments can be affected by malware such as remote-control Trojan programs, viruses, worms, and botnets, citizens seem to bear the brunt of this criminal activity. Today, cyber viruses and worms use sophisticated techniques to propagate themselves. Whether through SPAM email with malicious attachments and the clever use of social engineering (http://blog.globalknowledge.com/technology/security/hacking-cybercrime/social-engineering-how-hackers-hack-the-human/), or traveling across computer networks and the Internet, attacks by self-replicating software such as Viruses and Worms are at an all-time high.

Crimes against Individuals, Businesses, and Governments

SPAM email, infected files on "free download" sites, malicious websites with pernicious pop-ups, and legitimate websites that have been poisoned by hackers also serve up malware. Remote-control software, called Trojans in honor of the story of the Peloponnesian Wars, hijacks users' legitimate systems for criminal purposes. Organized crime groups can then use these victims’ computers to steal data from a user or to commandeer the system to launch further evil deeds.

On an individual basis, hackers can then steal personal data from the infected computer such as bank account, login and credit card information, or they can use the system to launch DoS attacks or propagate SPAM. That SPAM, in turn, is used to further distribute malware, carry out illegal sales activity (such as pharmaceutical sales), or to launch further DoS attacks.

Large-scale networks of hacked computers under the remote control of criminal enterprises are often called Botnets; the victims called Bots or Zombies (mixing metaphors.)

Governments, businesses, and individuals are now experiencing a new type of attack that the press calls "Ransomware." This Cryptoviral Extortion (ed.: cf: http://www.techrepublic.com/resource-library/whitepapers/cryptoviral-extortion-a-virus-based-approach/) often occurs when a user navigates to a malicious website and then clicks on a poisoned pop-up box or the victim experiences a "drive-by download." These Trojan programs then encrypt the victim's personal or corporate data and extort a payment (often One Bitcoin) for the key to release the information.

For businesses and governments, direct cybercrime takes the form of attacks against web servers and the databases that support the organization's sites. Websites are subject to attacks such as DoS and defacement. Stealing information such as usernames, passwords, PII, or credit card information provides lucrative fodder on the Internet black market.

Press reports in mid-November 2014 included reporters quoting testimony by the head of the CIA that he believed the nation's critical infrastructure was vulnerable to attack by nation-states and terrorist organizations. In other words, cyber-war is a large concern for many.

As a side note, not-for-profit organizations such as religious groups, charities, and such face the same challenges. With these groups, I'll also include non-governmental organizations (NGOs), which can also become cyber-targets. Such organizations are not immune to attack simply because of the nature of their work.

Internet Service Attacks

Because websites and other Internet-facing services are thoroughly integrated into our lives, attacks on companies, governments, and even individuals occur through what we used to call the Information Superhighway. When we used that anachronistic term, we weren't as nearly dependent on the "web" as we are now.

Using the analogy of a workers' strike that inconveniences business' customers to propagate the strikers' message with the hope of pressuring consumers to respond to the business, Internet service attacks pose most problems for users of those services.

Website defacement, more so, and DoS attacks affect both the company or government and the Internet-based users of those services. If a consumer can't access an organization's resources or they are greeted with a hacktivist message, the point is made.

Individuals and business can also have their Internet presence hijacked. Whether it's someone breaking into the Associated Press Twitter account, hacking the personal and corporate data of security firm HBGary, a DoS attack against the New York Times, or having a Facebook account usurped, these incidents are all directed at individuals. The Sony data breach of November 2014 demonstrates how effectively the attackers can act.

Sony, as well, brings us to the gray area of cyberwar and cyberwarfare. As I'm writing this, the FBI and popular opinion lay blame on North Korea, but there is a great deal of skepticism in the cybersecurity community. Part of the problem with cyberwarfare is definition—what does it mean to have a cyberwar attack? Another part is attribution—who did it needs to be separated from glorification, or who *says* that they did it.

Indirect Cybercrime

With the exception of hacktivism, there are usually secondary motives to cybercrime. They may include governmental attacks one-against-the-other, monetizing stolen information, espionage, or hijack of legitimate systems to carry out the attacks. Often, as in the case of systems with a Trojan or a Bot, many of these are blended in the attack.

Personal

Individuals and families have long been targets of financial and related fraud. The theft of credit card numbers in 2013 and 2014 was largely for the purpose of selling the stolen information so other criminals could "cash out" whatever value they had. Perhaps one of the best sources for information on the "year-of-data-breaches" comes from Brian Krebs - http://krebsonsecurity.com - his book *SPAM Nation* is recommended reading.

To illustrate the severity of the problem, I contacted my bank to see if they could send me a new credit card with EMV (Europay, MasterCard, and Visa—Chip-and-Pin) technology. Speaking to the customer service representative, the agent said that they could not because the bank was dealing with reissuing cards for all of the victims of the Home Depot cyberattack.

To me, while identity theft and fraud from stolen financial information are related, the purpose of these cybercrimes is different. With identity theft, the criminal is trying to impersonate the victim. The goal of the impersonation is use the victim's reputation and credit history as their own to obtain a loan, credit card, make a purchase, or "become" the other person and hide their own real identity. Financial and related fraud simply take a person's information (such as a checking and debit account numbers) and use that to make purchases or withdraw money from bank accounts—often with manufactured fake credit/debit cards or other similar mechanisms.

Personal information can often be stolen from trusted third-party sources. For example, when a website's user database and related passwords are stolen, then the cybercriminal can try to log into the same site or others. The latter works because people often use the same user names (or may be required to give email addresses) and recycle their passwords. Other forms of information stolen from trusted third parties often come from SPAM-related attacks; either when a user clicks on a malware-infected attachment, clicks on a malicious web link, or is enticed to enter login information to what appears to be a legitimate site such as a bank (but really isn't.)

Lastly, tax and healthcare/medical fraud cost billions of dollars. Demos.org estimates that tax fraud has cost the US Government $3 trillion—with a "T"—in the past decade. The FBI estimates that the amount of healthcare fraud is in the "tens of billions of dollars per year." Through identity theft (a patient pretending to be someone else), fraudulent transactions from caregivers, and drug crimes, cybercriminals are using stolen information to commit the bulk of these crimes.

In all of these cases, the individual is left the work and cost of cleaning up the aftereffects. These include damage to credit reports, possible lawsuits, and loss of reputation.

Commercial

Businesses need to protect their proprietary information in a number of dimensions. Looking at the use of stolen data, cybercriminals seek out trade secrets, product plans —both present and future—and other information that can help competitors gain advantage. As I mentioned earlier, this was a key element of the Department of Justice's indictment in May 2014. Business-against-business hacking seems rare, with the exception between organized crime groups. On the other hand, companies' proprietary product information can be sold to unscrupulous businesses.

Other proprietary information includes customer data, credit card numbers and other purchase information, and employee details. Because healthcare fraud is rampant as well, PHI must be protected even if an organization does not meet the criteria for a so-called "covered entity" under HIPAA.

Looking at the risk to businesses, there are essentially two threat sources: the outsider and the insider. Over the last year, the hacks upon major retailers, hotel chains, and other businesses have come from organized crime groups rather than from disgruntled or compromised staff or former employees.

Most spectacularly, Bradley (now Chelsea) Manning and Edward Snowden's information disclosures were from the inside of their organizations. While both of these occurred in a military context and divulged diplomatic or intelligence information and capabilities, these are demonstrative of the risk to an organization from within its walls. For example, AT&T suffered two insider data breaches in June and August 2014. These allowed access to customer information, social security and driver's license numbers, and dates-of-birth.

Commercial organizations must also worry about subversion of their networks and systems: in his blog, Brian Krebs identifies the names of servers that were hijacked in the cause of stealing credit card numbers and other information from Target Corporation.

At the time this is being written, the Sony data breach is unfolding. News reports about the incident discuss possible North Korean involvement, as well as scripts to upcoming movies and the disparaging nature of disclosed email messages. Security pundit and noted cryptographer Bruce Schneier points out that the largest group of victims may be Sony employees because of leaked financial, personal, and medical information.

Governmental

For most national governments around the world, both civilian and military organizations depend heavily on their communications and computational infrastructures. Cyberattacks for the purpose of delivering crippling blows, in the case of warfare, or espionage, are both the tools of statecraft and hacktivism. The purpose of the *Conficker* attack of late 2008 was to propagate a botnet used both as a Trojan and as a DoS tool, successfully infecting missions of computers including those in the US Military Central Command and resulted in the banning of the use of USB sticks within American Armed Forces networks. Six years later, the *Regin* spyware tool performs similar cyber-espionage attacks. In an ongoing battle, governments around the world both defend against and use such software for intelligence gathering purposes.

The term "cyberwar" has been used in connection with the Sony data breach, although most of the cybersecurity community avoids the term. On the other hand, an attack against a country's critical infrastructure or the DoS attacks against the country of Georgia may rise to that level.

State and local governments are less targets of warfare and espionage than they are of other attacks such as data theft, DoS and website defacement. In that respect, they more resemble businesses and commercial organizations in their security needs and posture.

Hacktivism

Hackers who perform their attacks for social, religious, political, or philosophical causes inflict their harm on both the direct target and also secondary victims. A company or governmental organization may find their website defaced or unavailable due to a DoS attack. The cost to diagnose the hack, repair the damage, and prevent future attacks can be substantial for an organization.

Hacktivism, however, also has secondary victims, ranging from the consumer who cannot use web resources because of the attack to individuals whose privacy or confidentiality has been breached.

Commenting on the Sony data breach, President Obama called the attacks cyber-vandalism, echoing what we emphasize in the introductory chapter of the Certified Ethical Hacker class (CEHv8). (http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=20241&country=United+States)

No matter the motivation of such hacks, the outcomes are hurtful and the actions criminal.

What Can You Do?

Whether we want it or not, our lives are twined to the Internet and electronic systems. We will divulge information about ourselves by registering to gain access to web services, we will participate in social networks, and we take functions such as online banking and web services such as email as commonplace.

Even if we limit or abstain from deliberate online activity, we are part of the Internet ecosystem because of interactive functions such as electronic health records (EHRs) and the records business keep about our purchases.

As much as we'd like to be able to go "dark" and disconnect electronically, it is infeasible and potentially illegal. That means that traces of our lives exist in computer systems and networks over which we have no control.

There are, however, actions we can take to help reduce the vulnerability and mitigate the impact of hack attacks on others.

Personally, we can limit the information that we give out. For example, I have a Facebook account that I only use to access pages that require me to login. Daily, I get an email with the subject line, "You have more friends on Facebook than you think," which offers to have me upload my email address book and then the service can scan its database for me. Please allow me to be colloquial, but, "Not only NO, but [expletive] NO!" I also eschew websites that require me to register to view information in which I bear only marginal interest. A famous author's website comes to mind.

In his excellent post on Global Knowledge's Blog Site, James Michael Stewart writes about "Top 5 Risky Internet Behaviors" (http://blog.globalknowledge.com/technology/security/hacking-cybercrime/top-5-risky-internet-behaviors/) and how to protect yourself. Likewise, I have a pair of articles on dealing with SPAM: "Signs an Email is SPAM" (http://blog.globalknowledge.com/technology/security/hacking-cybercrime/signs-an-email-is-spam) and When a Friend “Sends” You Junk Email" (http://blog.globalknowledge.com/technology/security/hacking-cybercrime/when-a-friend-sends-you-junk-email/). All good advice.

There is little we can do to disconnect ourselves from the electronic financial system. As a result, standard suggestions will have to suffice:

First, check your bank and credit cards regularly and meticulously. Ironically, this means that you will have to use the same systems that possibly make you vulnerable.

Secondly, check your credit reports regularly. There are many online services to help you, which is again ironic. There's at least one free service (paid by their advertisers) that allows you to look often and updates monthly.

Use a credit card where and when you can. In my blog "Online Shopping, Credit Card Fraud, Identity Theft, and You" (http://blog.globalknowledge.com/technology/security/hacking-cybercrime/online-shopping-credit-card-fraud-identity-theft-and-you/), I talk about financial protections for transactions.

Lastly, if you have been a victim of one of the many data breaches and credit card information thefts in the last year, take advantage of the free credit protection that the companies are offering.

Conclusion

Hacking and hackers have been around since the beginning of the use of computers, although the term has only been in the parlance with negative connotations since about 1983. Informally, a "cool hack" usually referred to a particularly clever segment of computer programming code.

Today, we talk about "Black Hat" and "White Hat" hackers, and cybercrime is the province of both. The Black Hats attack and the White Hats defend. In my Cybersecurity Foundations class (http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=13526&country=United+States), we dissect several case studies related to cybercrime. As well, the focus of the Computer Hacking Forensic Investigator (CHFI) v8 (http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=23732&catid=191&country=United+States) is on the analysis and investigation of computer incidents including cybercrime.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

Cybersecurity Foundations

Computer Hacking Forensic Investigator (CHFI) v8

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Bob Withers is a Principal Consultant with BWA, Inc., a cybersecurity training and consulting company specializing in healthcare security. He is also a Master Trainer for Global Knowledge, teaching both cybersecurity and Microsoft curricula. Bob holds the CISSP certification from ISC2, C|EH, E|CSA/LPT, C|HFI, and C|EI certifications from EC Council, MCSE, and MCT accreditation from Microsoft, and many other industry-standard certifications. With more than 30 years of information technology and cybersecurity experience, Bob is also an author and speaker at security conferences across North America.