Trends in Cybercrime

Cyber crime is becoming more sophisticated in planning and organization
Viruses can affect computers around the world much more quickly than in the past
Code Red was a computer worm observed on the Internet in July 2001. It was identified when computers running on the Internet Information Services (IIS) web server of Microsoft were found compromised. The after effect of the attack caused billions of dollars of damage in the summer of 2001. Code Red infected 150,000 computer systems in 14 hours.
Although the worm had been released on July 13, the largest group of infected computers was seen on July 19, 2001. On this day, the number of infected hosts reached 359,000.
A Windows 2000 machine infected by the **Code Red II** worm no longer obeys the owner. That's because the worm creates a backdoor into the computer's operating system, allowing a remote user to access and control the machine. In computing terms, this is a system-level compromise.
First appearing in September 2001, **Nimda** is a computer virus that caused traffic slowdowns as it rippled across the Internet, spreading through four different methods, infecting computers containing Microsoft's Web server, Internet Information Server (IIS), and computer users who opened an e-mail attachment. Like a number of predecessor viruses, Nimda's payload appears to be the traffic slowdown itself - that is, it does not appear to destroy files or cause harm other than the considerable time that may be lost to the slowing or loss of traffic known as denial-of-service and the restoring of infected systems. With its multi-pronged attack, Nimda appears to be the most troublesome virus of its type that has yet appeared. Its name (backwards for "admin") apparently refers to an "admin.dll" file that, when run, continues to propagate the virus. It spread through 86,000 computers in 1 hour.

Slammer is a 2003 computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic. It spread rapidly, infecting most of its 75,000 victims within 10 minutes. It caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic. Bank of America's ATM service crashed, the city of Seattle suffered outages in 911 service and Continental Airlines had to cancel several flights due to electronic ticketing and check-in errors. By some estimates, the virus caused more than $1 billion in damages before patches and antivirus software caught up to the problem. The progress of Slammer's attack is well documented. Only a few minutes after infecting its first Internet server, the Slammer virus was doubling its number of victims every few seconds. Fifteen minutes after its first attack, the Slammer virus infected nearly half of the servers that act as the pillars of the Internet. Slammer exists entirely in the computer's memory. At no point does it save itself to any disk. It makes no changes to the system at all. These facts make removal of the worm as easy as shutting the system down.

Polymorphic malware is a type of malware that constantly changes its identifiable features in order to evade detection. Many of the common forms of malware can be polymorphic, including viruses, worms, bots, trojans, or keyloggers. Polymorphic techniques involve frequently changing identifiable characteristics like file names and types or encryption keys to make the malware unrecognizable to many detection techniques.

Polymorphism is used to evade pattern-matching detection relied on by security solutions like antivirus software. While certain characteristics of polymorphic malware change, its functional purpose remains the same. For example, a polymorphic virus will continue to spread and infect devices even if its signature changes to avoid detection. By changing characteristics to generate a new signature, signature-based detection solutions will not recognize the file as malicious. Even if the new signature is identified and added to antivirus solutions' signature database, polymorphic malware can continue to change signatures and carry out attacks without being detected.

For example, the **Storm Worm Email** sent in 2007 with the subject "230 dead as storm batters Europe" was, at one point, responsible for as much as 8% of all global malware infections. When the message's attachment is opened, the malware installs trojan onto the recipient's computer, transforming it into a **bot**. One of the reasons the storm worm was so hard to detect with traditional antivirus software was the malicious code used morphed every 30 minutes or so.

Intelligent malware refers to hacking tools that are much more powerful and easier to use then in the past. This malware seeks out vulnerable systems and covers its own tracks.
As artificial intelligence is developed, it will sooner or later find its way into various malicious software. This could hold disastrous results for businesses and individuals who are the hackers' potential victims.
Artificial Intelligence (**AI**) is the branch of computer sciences that emphasizes the development of intelligent machines, thinking and working like humans. For example, speech recognition, problem-solving, learning and planning. The term is used to refer to machines which mimic human cognition. At least some of the things we associate with human minds, such as learning and problem solving can be done by computers, though not in the same way as we do. It has also been defnied as a system's ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation.
Smart viruses have the ability to hold industrial or government equipment for ransom. Mixing AI with ransomewhare could turbo-charge these attacks and enable them to spread automatically to new targets.
Smart viruses will learn to act like humans. Using neural networks, it is already possible to mimic the writing style of a person. With just a few samples of text, smart viruses can learn to mimic a writer in order to infect other people in his/her circle, posing as the writer.

To demonstrate the danger of AI-powered malware, researchers at IBM armed DeepLocker (an attack tool powered by artificial intelligence) with the popular ransomware WannaCry and integrated it into an innocent-looking video-conferencing application. The malware remained undetected by analysis tools, including antivirus engines and malware security programs. Hackers can use AI to help their malware evade detection for weeks, months, or even years, making the chances of infection and success skyrocket.

While running, the application feeds camera snapshots to DeepLocker's AI, which has been trained to look for the face of a specific person. For all users except the target, the application works perfectly fine. But as soon as the intended victim shows their face to the webcam, DeepLocker unleashes the wrath of WannaCry on the user's computer and starts to encrypt all the files on the hard drive. Other means through which AI could identify an individual include voice recognition and geo-location.

Malicious actors can also tune the settings of their AI-powered malware to target groups of people. For instance, hackers with political motives might want to use the technique to hurt a specific demographic, such as people of a certain race, gender or religion.

In recent months, publicly available AI tools have been used to produce offensive content on the Internet. At the beginning of the year, a Reddit user called deepfakes used simple open-source AI software and consumer-grade computers to create fake porn videos featuring celebrities and politicians. The outbreak of AI-doctored videos and their possible repercussion has become a major concern for tech companies, digital rights activists, lawmakers and law enforcement.

These programs do not require the use of human interaction and constantly work without stopping for a break. Along the way of causing chaos, the malware has the ability to move fast, adapt, change, and learn from the programs trying to remove it, only becoming stronger and harder to get rid of.

Ransomware will be a big target with smart technology, as AI will only make it easier to ransom devices and networks.

IoT devices, such as medical devices, will most likely be the target for these attacks and the assets and data behind them.

The smart malware will also disguise itself as phishing malware; learning and imitating the user's writing and communication style to send false email messages targeted to infect other users or organizations. Smart phishing malware will be seen soon, as there are already existing technologies like Google DeepMind that have natural speech and language tools.

Scareware is a malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection. These may appear as pop-ups claiming to be legitimate warnings from antivirus software companies, and they claim your computer's files have been infected.
In this scam, cybercriminals attempt to gain access to your credit card information, and often your computer itself, by tricking you into buying fake antivirus software.

Concealment: Encryption

Encryption software tools are computer programs used to protect sensitive or confidential data by converting it to a form that cannot be read by humans or computers without access to a numeric key that can restore the data to its original form. As long as the key remains confidential, encrypted data can safely be stored or transmitted without fear of being intercepted and disclosed to an unauthorized person or entity.

Encryption software is already deployed by some large corporations and government agencies to protect data, but it's also available and now accessible for a wider range of users, including hackers and cybercriminals.

[Remember that encryption is the process of converting information into an unreadable form by scrambling and overwriting the data; once encrypted, the information can only be converted back into readable form via an encryption key.]

Encryption provides cybercriminals with a technique for concealing the fruits of their criminal activity or the criminal activity itself. Once a fraudster has encrypted his/her criminal work, only people with a proper encryption key can view it.

Anonymity

A popular technology for concealing one's identity on the Internet is the TOR browser. The letters stand for "The Onion Router". It is a network of 5,000 relays around the world. Data is encrypted several times and sent through a randomly selected set of relays before being decrypted and delivered to the user.

The TOR browser isolates each website the user visits so third-party trackers and ads can't follow him/her. Any cookies automatically clear when the user is done browsing. So will his/her browsing history.

TOR browser prevents someone watching a user's connection from knowing what websites he/she visits. All anyone monitoring the user's browsing habits can see is that hs/she is using TOR.

TOR browser aims to make all users look the same, making it difficult for a user to be fingerprinted based on his/her browser and device information.

Traffic is relayed and encrypted three times as it passes over the TOR network. The network is comprised of thousands of volunteer-run servers known as TOR relays.

Cybercrime Commercialization

Cyber crime trends evolved from the typical “hackers” wearing a hoodie in dark basements to the smartly dressed fellow you pass in the streets. Anyone with access to Google and a few dollars can get involved in the lucrative illegal trade thanks to the commercialization of the industry. Recent research indicate that year-to-date global ransomware damage cost exceed $ 5 billion with *Wannacry* contributing highly to the cost. The cost is not only the cost of paying ransom but includes cost of recovery, incident management and implementing controls to prevent future attacks.

Cyber crime-as-a-Service (CaaS) is gaining popularity given the low investment and high return from the ‘business venture’. With as low as $7 and access to the dark web a novice cyber criminal can be buy malware that can be successfully launch a cyber attack on intended victims. Cyber crime has become a full-fledged commercial industry operating like any other services industry. The cyber criminal builds a malware then licenses it to interested parties (think of a distribution channel), then the partners can market the malware and earn commissions and pay royalties back to the owner of the malware. Police estimate that just 100 to 200 people may be powering the "cybercrime-as-a-service" ecosystem by developing the attack code and services that enable criminals who lack technical acumen to pay for their cybercrime to be accomplished.

Over the past 20 years, cybercrime has become a mature industry estimated to produce more than $1 trillion in annual revenues. From products like exploit kits and custom malware to services like botnet rentals and ransomware distribution, the breadth of cybercrime offerings has never been greater. The result: more, and more serious, forms of cybercrime. New tools and platforms are more accessible than ever before to those who lack advanced technical skills, enabling scores of new actors to become cybercriminals. Meanwhile, more experienced criminals can develop more specialized skills knowing that they can locate others on the darknet who can complement their services and work together with them to come up with new and better criminal tools and techniques.

There are plenty of ways for a cybercriminal to make money without ever perpetrating "traditional" cybercrime like financial fraud or identity theft. The first way is something called research-as-a-service, where individuals work to provide the "raw materials" — such as selling knowledge of system vulnerabilities to malware developers — for future criminal activities. The sale of software exploits has captured much attention recently, as the ShadowBrokers and other groups have introduced controversial subscription programs that give clients access to unpatched system vulnerabilities.

Exploit kits are another popular product on the darknet. They provide inexperienced cybercriminals with the tools they need to break into a wide range of systems. However, Europol notes that theft through malware has general becoming less of a threat; instead, today's cybercriminals prefer ransomware and distributed denial-of-service (DDoS) extortion, which are easier to monetize.

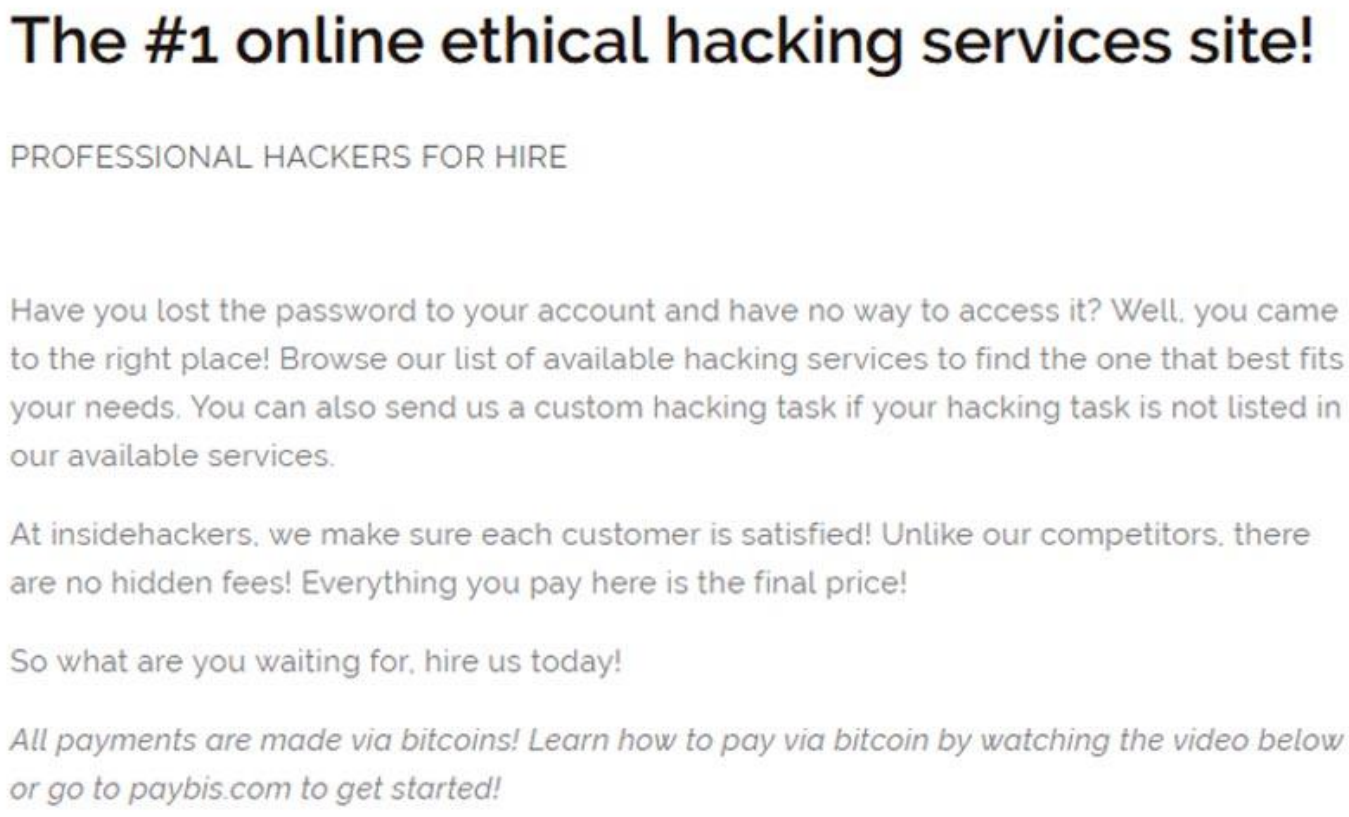
Hackers can profit from more sophisticated cybercrime by providing cybercrime infrastructure-as-a-service. Those in this field provide the services and infrastructure — including bulletproof hosting and botnet rentals — on which other bad actors rely to do their dirty work. The former helps cybercriminals to put web pages and servers on the Internet without having to worry about takedowns by law enforcement. And cybercriminals can pay for botnet rentals that give them temporary access to a network of infected computers they can use for spam distribution or DDoS attacks.

Hackers-for-hire

In recent years, it has become easier than ever for anyone who has the necessary financial resources to tap into the "hacker-for-hire" market. It's as straightforward as searching through Google results.

There, people can find hacker marketplaces where participants promote their skills and sometimes provide their price ranges. Initially, many hackers for hire only operated on the dark web, but now their services are so in demand that broadcasting them is commonplace.

Most hackers for hire work anonymously, and their rates go up depending on the complexity of a hack and how long it takes to do. It's possible to hire a hacker for as little as $5 per hour, meaning the option is open even to those with minimal financial resources. Some of them also prefer Bitcoin payments rather than traditional currencies. People who are successful hackers for hire generally know various programming languages. They are also extraordinarily detail-oriented and capable of working efficiently under pressure.
Here is an actual advertisement for a hackers-for-hire organization:



Integration of Cybercrime(s)

This graphic is meant simply to illustrate that, like many terrestrial crimes (criminal homicide, robbery, larceny-theft, etc.), a cybercriminal incident involves more than one offense- the specific individual offenses are integrated into a single criminal event.

The scenario in the graphic on the preceding page unfolds something like this:

Step 1: [Phishing] The thief sends an email with a link or attachment to the victim that appears to come from a known party. The targeted victim then clicks the link or attachment, which includes malicious software (malware) that infects the victim's computer.

Step 2: [Spyware] The thief uses installed malware to steal login credentials to the victim's financial accounts. This will generally allow the thief to log in as the victim.

Step 3: [Fraud] With access to accounts, the thief changes the victim's profile at the financial institution and/or impersonates the victim and moves money to criminal accounts at a different institution.

Note that this one event- which would probably be classified as a fraud- also entails two other forms of cybercrime- phishing and spyware.

The trend in cybercrime now is for more criminal events to integrate several other cybercrimes in the same incident.

Organized Cybercrime

Many people still picture basement-dwelling loners when they think of a “cybercriminal,” however, the reality is that modern large-scale cybercrime looks far more like a corporate enterprise than we’d like to imagine. Not unlike drug cartels, cybercrime rings are more agile, more efficient, and oftentimes more organized than the security experts working to stop them.

Like a standard enterprise, a cybercrime ring typically adheres to a clear organizational structure, one with well-defined roles and an agreed upon chain of command. At the top will be an organizational **leader**, an individual responsible for conceiving of and planning each cyberattack and ensuring that every person below them understands their role and communicates effectively both up and across the chain of command.

Cybercrime rings also almost always have a **team of in-house programmers** who are tasked with developing new variations of malicious software capable of infecting targeted systems, spreading quickly and widely, and most importantly, evading detection. According to McAfee Labs’ 2018 Threats Predictions Report, the total amount of known ransomware alone grew by 56% last year. That shows just how dedicated cybercriminal rings are to creating malware that’s more dangerous, less visible, and harder to stop than what their targets are expecting.

The next two roles — network administrators and intrusion specialists — often operate in tandem and are the critical players while an attack is taking place.

A **network administrator** manages their ring's full slate of malicious payloads (viruses, ransomware, denial-of-service attack packets, etc) deciding which "tool" to use and which moment represents the best opportunity to launch the attack.

An **intrusion specialist**, on the other hand, is charged with making sure that any and all malicious software that is successfully installed on the target's systems continues running for as long as possible.

Finally, in order to guarantee that their scheme ends up being profitable, cybercrime rings employ both data miners and financial specialists.

Data miners organize and reformat stolen data in order to make sense of it.

Financial specialists determine how much money the specific information they've stolen is worth on various black markets.

Unfortunately, taking down any one of these team members doesn't necessarily compromise the entire crime ring. For one, cybercriminals often prefer to give and receive compensation in the form of untraceable cryptocurrencies like Bitcoin. This effectively eliminates the "paper trails" that have undone criminal organizations in the past.

What's more, cybercriminals are careful to only share incriminating information on the Deep Web (a term that refers to all the online content that is not indexed by traditional search engines) where anonymity is easily achieved. Many cybercrime rings "subcontract" various roles to anonymous individuals they find in these "hidden" corners of the internet, greatly reducing the likelihood that any one person knows enough to harm other team members.

Juvenile Cybercrime

Cyberbullying is a common for of juvenile cybercrime.

Another of the most common online offenses committed by juveniles is "digital piracy" - sharing and/or downloading of software and digital music and movies without the permission of the copyright holder. According to a study that appeared in the journal *Psychology, Crime and Law,* most college students don't consider such downloading to be stealing and don't believe it's morally wrong. There are probably a number of reasons for this:

The intangible nature of digital "goods" is different from that of tangible goods. Traditionally, the crime of theft involved "unlawfully appropriating property without the effective consent of the owner, *with the intent to deprive the owner of the use of the property*." When you download a copy of a song, you don't deprive the owner of the use of that song, as you do when you steal a tangible item. Kids have a hard time understanding such abstractions.

The corporate nature of most of the copyright holders means kids don't see themselves as taking something that belongs to another *person* (regardless of the law's treatment of corporations as persons for some purposes), but from a huge, nameless, faceless entity. The belief that these corporate copyright holders are unethical, greedy and immoral means that even if they did see it as stealing, kids (who generally love Robin Hood stories) would find it more acceptable to steal from those who, in their eyes, are evil.

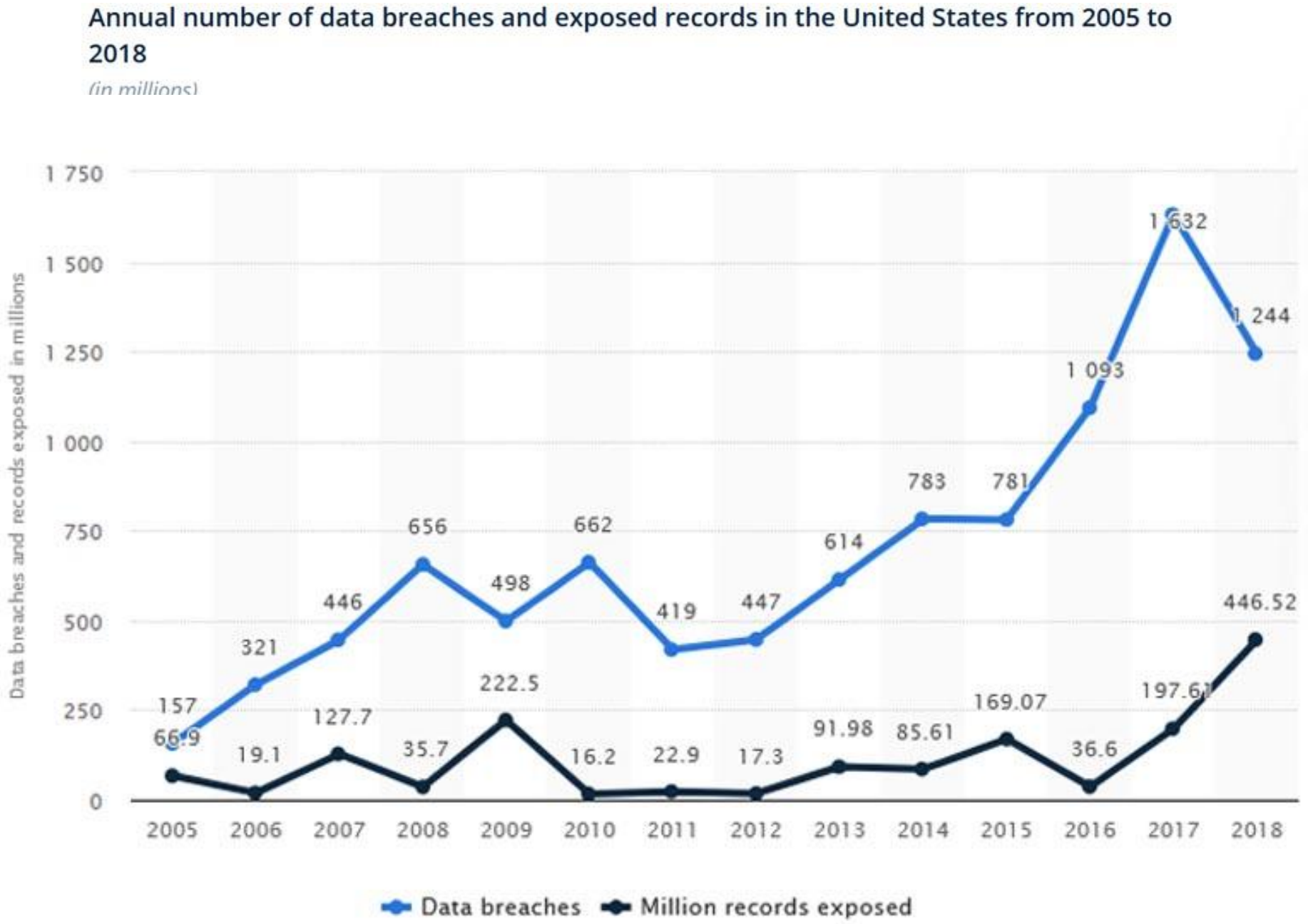
the penalties are much steeper.

Another common juvenile cybercrime is viewing or swapping of pornographic material. This is a case (unless it involves underage models/actors) of an act that is illegal for juveniles but becomes perfectly legal on one's eighteenth birthday. A profound interest in sex is a part of human nature and teenagers are awash in hormones that make this "crime" almost an inevitability, given the temptation of all the easily available porn on the Internet.

Criminal trespass via computer (which most laws call *unauthorized* access) is another of the most common juvenile cybercrimes. The stereotypical hacker is a nerdy teenager who breaks into remote systems not for the purpose of stealing and using information, and often not even for the purpose of creating havoc, but merely to prove to himself and others that he has the skills to do it. In some cases, however, that teenager can be prosecuted under the same laws (and sentenced to the same penalties) as a terrorist who hacks into systems to disrupt vital communications with the intent to cause serious injury and death.

Some kids go further and, when they gain access to other systems and sites, want to do damage to leave their mark behind - much as their fathers and grandfathers expressed their teenaged angst by demolishing mailboxes or spray-painting graffiti on walls. The difference is that this cybervandalism can cost the victimized companies or individuals much more, and consequently the penalties are much steeper.

Threat to Privacy



10 Privacy Threats

1. Vulnerabilities in Web Applications

A single vulnerability is more than enough to cause a major data breach.

2. Insiders and Poorly-Trained Employees

Data exposure on the operator side is caused either intentionally by a malicious insider or unintentionally by a simple mistake.

3. Lacking Breach Response

Even with the best security controls, incidents leading to leaks are still a possibility. The point here is to beprepared to provide a swift response to minimize the impact of unforeseen situations.

4. Inadequate Personal Data Disposal

Personal data should be kept only as long as the relationship with the customer or employee (and related legal obligations) are in effect

5. Lack of Transparency in Privacy Policies, Terms and Conditions

Consent is a major requirement for collecting, storing or processing personal data. In principle, in order to consent to something, it is first necessary to be able to understand what you are consenting to. Many companies still fail to publish a proper privacy policy.

6. Collection of Unnecessary Data

Collecting data should always be done with a specific purpose for which consent has being received.

7. Personal Data Sharing

To put it simply, data is a currency, and it is quite common for companies to share it with third parties for several reasons. These reasons can range from enabling simple website widgets (e.g. maps, social networks buttons), to monetary compensation and political schemes.

8. Incorrect or Outdated Personal Data

Individuals have the right to rectify outdated or uncorrected personal data. This ranges from a simple address update to more complex situations, such as a medical record.

9. Session Expiration Problems

Let's say an individual gave consent for data collection while using an online service. If this service fails to implement measures such as a logout button or automatic session timeout, this may result in collection of additional personal data without the user's consent or awareness. Some services do not implement automatic session expiration, and if a person forgets to log out and leaves the computer unattended, someone else could easily have access to personal or even sensitive information.

10. Data transfer Over Insecure Channels

Personal data being transmitted over insecure protocols (e.g. FTP, HTTP) can be easily captured by an unauthorized third party. For this case, enforcing secure protocols (e.g. SFTP, TLS) is the safest option for avoiding a breach.

In addition to these 10 threats, many vulnerabilities can remain dormant for several years before being discovered and causing a major privacy impact. This vulnerability plagues most modern processors, affecting personal computers, mobile devices and even cloud infrastructure. It allows attackers to steal data, including personal information.