Solving the cybercrime problem

By John Bandler, Esq., Bandler Law Firm PLLC

MARCH 21, 2023

Cybercrime is no longer a new problem, but we still struggle to deal with it. Our solution starts by acknowledging how government can do more.

Cybercrime is costly to our economy, organizations, and individuals. No one is immune from these threats which steal, disrupt, affect our peace of mind and even national security.

We are united in seeing cybercrime as a serious harm but divided in understanding what it is and how to address it.

Cybercrime defined — let us break it down

"Cyber" has been appended to dozens of words, but cybercrime is the most important and cybersecurity next. Because of the first, we need the second.

We are united in seeing cybercrime as a serious harm but divided in understanding what it is and how to address it.

Cybercrime has two main components:

- **Cyber** essentially means using the internet and a computer (today's computers are almost always connected to the internet).
- **Crime** means there is a criminal law against it.

Therefore, cybercrime is basically a crime using the internet and a computer.

Some might distinguish between "cyber enabled crime", "cyber dependent crime" and "cyber native crime". Or among cybercrime, computer crime, internet crime and traditional crime.

But we should start by recognizing most cybercrime is just theft.

An evolution of theft towards the cybercrime era

In many ways, cybercrime is just a step in the evolution of thousands of years of human history of stealing. An unfortunate but long human tradition.

If something is valuable, there is someone who wants to steal it. If a new tool is invented, someone will use it for illegal purposes.

Before we had formal laws, governments, or currency some early humans stole the valuables of the day: food, firewood, shelter, and land.

Societies have long tried to address these criminal acts, but never with perfect methods or results. Eventually criminal laws were created and a justice system to administer them. Goals have included prevention, deterrence, punishment, and rehabilitation, with shifting focus over the years.

Society, crime, and crimefighting have evolved. Some developments brought significant changes to theft and its investigation, including banks, firearms, and automobiles. As the 21st century approached, the next steps would be an explosion, even if the basic theme of theft remained.

The big bang of cybercrime

As we passed through the millennium there was a new ecosystem for theft. The internet formed and personal computers were everywhere. The credit industry boomed with a market for consumer personal information. The payment card business expanded with ever-present credit and debit cards. Anonymous internet payments became possible with virtual currencies and eventually cryptocurrencies ("Cryptocurrency past is prologue: before and after FTX," Reuters Legal News, Jan. 17, 2023, http://bit.ly/3mSB4OX).

All of this meant a new illicit market for personal and financial information, and the ability to steal and profit from a distance. A global economy of cybercrime and identity theft was born.

This illicit economy was investigated during a trailblazing case (*People v. Western Express International, Inc.*, *et al*, or The Western Express Case) by the New York County District Attorney's Office (DANY) under the legendary Robert M. Morgenthau. (The author, as assistant district attorney at the time, led this investigation which revealed global cybercrime, identity theft, money laundering, and the use of early virtual currencies).

Since computers and the internet are now part of all we do, they are also part of criminal methods and tools to victimize us.

What is different about cybercrime

Cybercrime comes with four main differences from traditional theft:

(1) **Distance**. Theft used to be local, but cybercrime means it can be interstate and international. The victim, suspect, law

enforcement, and evidence are no longer together within a jurisdiction.

(2) **Data** has value to commit identity theft, which means cybercriminals want to steal it. We value our own data, so cybercrooks also employ ransomware to lock up our data and extort us. Data breaches and ransomware are just theft by another name.

(3) **Anonymized payments** and money laundering are an integral part of cybercrime so virtual currencies and cryptocurrencies play an important role.

(4) **Investigative complexities** are greater. Cybercrimes require more investigation, techniques, witnesses and exhibits than traditional theft crimes. Prosecutors and law enforcement need to invest years to build people, processes, and the bigger cases. That can be a tough sell for some officials.

We cannot cybersecurity the cybercrime problem away

It is wrong to think that better cybersecurity will make the cybercrime problem go away. Cybersecurity is important but will never alone solve the problem.

Cybercriminals who try to steal are not deterred by cybersecurity. Cybercriminals know it takes many attempts to be successful. Unless there are consequences, they will keep trying and with different targets too. No society can fortify every potential victim and no defense is impenetrable forever.

Steel doors and high security locks slow burglars until the police come. Military obstacles slow attackers while the opposing soldiers defend.

But attackers are deterred only when they fear consequences. With cybercrime, that deterrence can exist only if government does better with criminal investigation and enforcement.

No, do not hire criminals

A misguided idea from a few is to offer cybercriminals honest jobs.

But offering a dishonest person a position of trust is never a good idea. Today's cybercriminal is not the thrill hacker of decades ago, where a few became legitimate cybersecurity consultants.

We do not hire career thieves as security guards, nor foxes to protect henhouses, so cyberthieves past and present should never guard our cyber assets.

The solution lies with government and proper investigation and enforcement

Cybercrime needs to have consequences which only government can bring. Most cybercrimes are not investigated at all, and most investigations go unsolved.

Imagine a victim calling their police department and being told it doesn't handle burglaries, robberies, or car thefts, or that the car wasn't worth enough to warrant an investigation. The analogy is not perfect, but the unfortunate fact is many reported cybercrimes are not investigated properly if at all. Many of those reported crimes are just the tip of an illicit iceberg. Without proper investigation there is no chance of solving the crime.

Investigation needs to follow the money to identify the cybercriminal and money launderers, and stem the flow to reduce financial incentives.

Many will disagree on what "justice" and "proper enforcement" mean in general and for specific cases. But even the softest of enforcement consequences is better than the current reality that most cybercrimes go unsolved.

We can bring more offenders to justice only with improved government action, better investigation and cooperation from state, local and federal authorities. Federal law enforcement has amazing capabilities but limited capacity and high thresholds to investigate and prosecute. State and local law enforcement do the bulk of criminal justice work in our country, and that can include more cybercrime investigation.

Many dedicated professionals in government are working hard for us, and we are lucky to have them. We can acknowledge and thank those individuals while recognizing government's need to improve.

International cooperation and pressure too

We need other countries to do their part to assist, to investigate cybercriminals within their borders and the funds that pass through.

We can improve how that happens through our full array of international tools including legal, diplomatic and economic. Sometimes a carrot, sometimes a stick.

The nation-state connection in the cyber realm extends past crime to the full range of national security issues, but that is beyond today's topic.

Next steps

We are now reliant on the cyber realm, our world is digital, and there is no going back.

Government's path against cybercrime is clear. Investigate cybercrime better, bring more wrongdoers to justice, staunch the flow of illicit profits. Without enforcement and deterrence, malefactors have free reign.

The direction for organizations is more limited. Build our cybersecurity to protect ourselves as part of good business management and to comply with legal requirements. For businesses and individuals, good cybersecurity needs to become a fact of life like putting on our seatbelt in a car and locking our front door at night.

Cybercrime is here to stay. Effective cybercrime investigation needs to get here too.

About the author

John Bandler is a lawyer, consultant, speaker, author, and adjunct professor at Elisabeth Haub School of Law at Pace University. He helps protect organizations from cybercrime, improve cybersecurity, and better manage information assets, and is the co-author of "Cybercrime Investigations: A Comprehensive Resource for Everyone" (CRC Press, 2020). His firm, based in New York, is **Bandler Law Firm PLLC**. He can be reached at JohnBandler@JohnBandler.com.

This article was first published on Reuters Legal News and Westlaw Today on March 21, 2023.