Financial Times

April 9, 2015 1:22 pm

Taking on the smart criminals

By Emma Jacobs



Photo: © Daniel Jones

In the mid-1990s, Marc Goodman, then an investigator in the Los Angeles Police Department, tried to convince his boss of the need for a computer crime unit. The reaction? Utter bafflement. “This captain said to me, ‘Computer crime, what is that? Like if you take the monitor and hit somebody in the head and kill them?’”

It is a telling anecdote. While law enforcement agencies have become increasingly sophisticated technologically, criminals have the edge, according to Mr Goodman. That was something he observed when investigating drugs and vice in LA. “In those days the only people that had pagers in the US were physicians. Then you’d start to see street dope dealers carrying pagers. I’m like, ‘You don’t look like a doctor.’”

Criminals are the true early adopters, says Mr Goodman. Synthetic biology, drones, artificial intelligence: the smart crooks are already on to it. “These people are really clever ... innovating technologies for fraud, financial gain or personal vendetta,” he says.

Drug cartels, he insists, are investing in research and development. “Crime Inc”, as he calls it, is hiring assembly-line workers from local aircraft factories to work in covert narco-drone plants in Mexico.

Criminal hackers are not isolated pimply youths of popular mythology tinkering about for fun, he says. They are older (40 per cent, he says, are over 35) employees of organised crime syndicates. According to the Center for Strategic and International Studies, the cost of cyber crime alone could be up to $575bn.

The 45-year-old, sporting glasses and an ill-fitting jacket, is a charismatic mix of geekish enthusiasm and quick-talking street smarts. He is on a mission to sell his book, Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It, which is why he is in London. But also to warn people to be more aware of privacy and security issues. Tech companies are not taking sufficient responsibility for their tools, he says.

As a child, his ambition was to become a cop and fight crime; robbers and swindlers — that kind of thing. With next to no tech skills, he could not have foreseen a stint at the Federal Bureau of Investigation as the resident futurist, eyeing nascent threats.

For a man who spends his working life speculating on future horror and disaster, Mr Goodman is remarkably cheery. He credits his happy disposition to an ability to switch off.

I tell him I found the book so terrifying that I had to stop reading it at night. The details and descriptions stalked my sleep. Babies are spied on over hacked webcams; assassins are booked via the dark web where one can also buy drugs such as “Devil’s Breath”, better known as scopolamine, which can wipe the memory of victims. Terrorists build robots to deploy bombs. It is a taste of what is to come.

More video

The future looks like hell. Hackers could hold people fitted with pacemakers to ransom, driverless cars could be commandeered from afar. Bio-criminals could create deadly viruses to attack populations or possibly one individual. The terrorists of today and tomorrow, writes Mr Goodman, may not have to worry about accessing controlled pathogens from government laboratories. “With the advent of synbio [synthetic biology], they can just download the genetic sequence blueprints and print these deadly viruses themselves,” he writes.

There is personal gain to be made from talking up future problems. Mr Goodman also advises government agencies on future crimes. “I’m not saying we need to worry about Martians landing on the United States, use my anti-Martian powder. These are already things that [are happening],” he insists.

In depth
As online threats race up national security agendas and governments look at ways of protecting their national infrastructures a cyber arms race is causing concern to the developed world

Further reading

Born in New York City, Mr Goodman joined the police force in New York just as it announced cuts. The LA police department came calling. “I wasn’t sure whether or not I wanted to go to California. A bunch of weirdos out there.” A recruiter gave him a choice: he could direct traffic in the snow or in shorts on Malibu Beach.

Once in Los Angeles, he discovered work was no beach party. “Things were nuts. Crime was through the roof. Vast amounts of violent crime, drug wars.” In 1992, the riots kicked off after police were acquitted of beating Rodney King. “What I realised during the riots is that the cops are only in charge as long as the people let them and when they decide you’re no longer in charge, you’re not.”

After participating in undercover operations in drugs and prostitution, he entered the world of high-tech crime by chance. He was the only one in the room who knew how to spellcheck in WordPerfect. In 1995 that was enough to mark him out as police techno-elite, and he was asked to investigate a hack into the police department’s own computer systems. The FBI was of little help, he says. “I called [the bureau] and here’s what I heard: ‘Hold on, hey Joey, do we got a computer crime expert? We don’t have one yet but we’ve got a guy going to school next year, can you call back?’”

In 1998, he set up a computer crime unit at LAPD. His skills have advanced since the early days, after studying computer forensics and gaining a masters in management of information systems at the London School of Economics.

The problem then, as now, he says, is that the internet has blown apart traditional policing, which is constrained by national jurisdictions. “Let’s say I wanted to do a search warrant in France, I have no authority. They’re under no obligation to co-operate.” Criminals, on the other hand, have no such restraints. Policing is not working, he says. “We’re using the wrong tools to fight it.”

Instead, he proposes public health organisations such as the World Health Organisation and the Centers for Disease Control and Prevention as models. “We talk about computer viruses, infections ... We should consider using the tools of medicine to combat the problem.” Instead of targeting individuals, the focus, he says, should be computer malware. “I’m guessing 0.001 per cent of cybercriminals are ever brought to trial.”

Today he works in the Singularity University, the private training centre in Silicon Valley founded by Ray Kurzweil, futurist and author, and entrepreneur Peter Diamandis. There he works with astronauts, roboticists and big data scientists to identify the possible dark side of innovation. He is also a script adviser for films he cannot yet discuss. Despite the razzmatazz, he says, his desire to spread doom and gloom is true to his police values of “protect and serve”.

“Technology is awesome, our future is going to be amazing, but it’s not going to come for free.”

emma.jacobs@ft.com

Twitter: @emmavj

Original article: Financial Times, April 9, 2015. Local archival reproduction prepared for MarcGoodman.com with permission. Original source URL: ft.com/content/806ac8f0-d7ac-11e4-849b-00144feab7de