# The Economy of Online Security

People who buy, sell, trade, or operate commercially online in a way that requests information from people, especially financial or payment information, are faced with a business landscape like the wild west of 1855. In that situation the money box was on a stagecoach pulled by a team of horses, and the coachman was accompanied by a handful of Pinkertons with long guns either riding with the driver on the stagecoach or alongside on horses, ready and willing to gun fight with mounted robbers who could appear anywhere on the route. The stagecoach is the online purveyor’s digital data traveling along a secure communication path. The Pinkertons are the digital security, some form of Captcha service or similar, and the money box is the secure data traveling the digital route. Nothing really changes at its core. Only the details change. The same basic human transactions continue. In this case the details have changed from the literal to the digital.

Let’s stay with our analogy. In the stagecoach scenario, the main worry is the size of the gang attempting the robbery and the quality and gauge of the firearms used. This is wwhat the Pinkertons might have referred to as tradecraft in the banditry profession. Usually the bandits were not as well armed as the Pinkertons, nor were they as proficient with the firearms, and, where quantity of capital being transferred and client resources permitted, deterrents like a Gatling gun could be engaged, mounted inside the stagecoach and hidden to the prospective robbers, and capable of scattering them to the four winds upon its deployment.

## The Contemporary Commercial Trade Route

Now let’s visit the contemporary digital banditry. The purveyor is responsible for the security, the Pinkertons. The buyer is somewhat responsible for their own security but mainly as it pertains to their financial information used to make the purchase. The transportation of the product, the digital trail, is the responsibility of the purveyor. The purveyor hires the Pinkertons, who, in the digital example, are security services like Captcha or other human verification technologies. The bandits are malicious coders who deploy various bots and other digital minions to attack the money box on the digital trail, and, just like the stagecoach trail, as the sophistry and numbers in the attacks increase so too must security. If the annual online security reports from various think tanks are to be trustworthy, and they are, it’s time for a digital Gatling gun. The level of sophistry in online attacks is growing at an exponential rate.

So much of what takes place online seems like it’s not real. Being online is the closest thing to interacting with people and being completely anonymous. It’s like a costume ball. You can go and interact with everybody and nobody is really sure of who you are. It emboldens people. The online world creates criminals who wouldn’t exist in the real world. In the stagecoach example the bandits required both criminal inclination and the metal to engage in a gun fight. The digital bandit needs only the criminal inclination. Throw in the political divisions in the West and many of the criminals can even convince themselves it’s morally Justified to rob large corporations. In the anonymous online digital world everybody is suddenly Charles Boles, known to most as Black Bart, the most prolific stagecoach bandit, operating from 1877 to 1883 and robbing twenty-eight coaches.

## Security is Reputation

The purveyor assumes the security costs, but more than the costs, they have the customer experience to worry about, their public reputation. There’s a lot at stake. The consumer wants expedience, and, aside from basic protection of their own data, assumes the digital trail is policed by the purveyor. What do you think would happen if the Amazon digital supply chain was hacked and stories started appearing in numbers of consumer data theft on the Amazon digital trail? Reputation is everything. But, too many hoops to jump through and many of the customers are just going to leave. They don’t quite understand that it’s for their own good. The ones victimized by online fraud get it, but the vast majority of potential clients will see security measures as a hassle. Purveyor tactics have to be simple, direct, and capable. Captcha was a tolerable middle ground between consumer expedience and purveyor reputation. It’s the human verification system endemic to the web now — select all the bicycles from a matrix of images — but the old methods of doing things are failing now. Digital bandits are combining artificial intelligence with bots to do things that can circumvent old style Captcha. It worked for quite a while, not so much anymore. In the old stagecoach allegory the simple laws of economy prevail. The Pinkertons could afford Gatling guns, not so the bandits. The real world lesson is economy is the requisite of security.

## Low Cost to Criminals

Coding is a zero cost economy outside of time and intellectual equity. Add to that organized crime and state sponsored actors bank rolling criminal software development and suddenly that Gatling gun advantage in the old economy goes away. What to do? It used to be that bots could only do one thing. It would show up and knock on your digital door. If you answered, it would walk through. If you didn’t answer, it would go away. Now they can do more. The democratization of artificial intelligence has made add-ons to bots simple and cost effective. It’s no longer just a one-off transaction like knocking on a door. Now the bot can ask if it can exhibit its wares. If declined the bot can now ask why and try to resell. The original merit of the bot as a tool for cybercrime was not its sophistry. It was the sheer volume of its deployment. The one-off transaction was rejected by ninety-nine percent of client systems, but the bots were so prolific that the one percent tallied into a viable income stream. Now there’s the dual threat of the prolific nature of the bots and the enhanced intelligence. There are bots out there now that can pantomime human behavior in a manner that will fool most security measures. There is no human response to the bot threat. It has to be digital. The sheer volume by which bots can be deployed makes a human response economically unfeasible.

As the forest firefighters say, you have to fight fire with fire, and where the two fires meet the burn stops. In this instance it means the solution is to deploy artificial intelligence (AI) and machine learning (ML) to meet the AI and ML of the criminals. Stop the steal the way the fire stops the fire. The old captcha programs no longer work, especially for high value targets. The criminal AI has learned how to game the image selection. A human verification system is needed, one that is simple, direct, and capable. Consumer convenience remains a concern. They cannot be labored with a long and drawn out access protocol, even if it’s for their own good. The consumer is impulse driven. If the security protocol is too exhaustive the impulse wanes, and if the impulse wanes the sale withers. This is the state of the digital economy. Meet the new economy, same as the old stagecoach economy, only less violent and dangerous but more costly and demanding than the simple solution the Pinkertons provided.