The Industrialization of CYBERCRIME

Lone-wolf hackers yield to mature businesses

Tamas Gaidosch

Cybercrime is now a mature industry operating on principles much like those of legitimate businesses in pursuit of profit. Combating the proliferation of cybercrime means disrupting a business model that employs easy-to-use tools to generate high profits with low risk.

Long gone are the legendary lone-wolf hackers of the late 1980s, when showing off level 99 computer wizard skills was the main reason to get into other people's computers. The shift to profit making, starting in the 1990s, has gradually taken over the hacking scene to create today's cybercrime industry, with all the attributes of normal businesses, including markets, exchanges, specialist operators, outsourcing service providers, integrated supply chains, and so on. Several nation-states have used the same technology to develop highly effective cyber weaponry for intelligence gathering, industrial espionage, and disrupting adversaries' vulnerable infrastructures.

Evolution

Cybercrime has proliferated even though the supply of highly skilled specialists has not kept pace with the increasing technical sophistication needed to pull off profitable hacks with impunity. Advanced tooling and automation have filled the gap. Hacking tools have evolved spectacularly over the past two decades. In the 1990s, so-called penetration testing to find vulnerabilities in a computer system was all the rage in the profession. Most tools available at that time were simple, often custom built, and using them required considerable knowledge in programming, networking protocols, operating system internals, and various other deeply technical subjects. As a result, only a few professionals could find exploitable weaknesses and take advantage of them.

As tools got better and easier to use, less skilled, but motivated, young people—mockingly called "script kiddies"—started to use them with relative success. Today, to launch a phishing operation—that is, the fraudulent practice of sending email that appears to be from a reputable sender to trick people into revealing confidential information—requires only a basic understanding of the concepts, willingness, and some cash. Hacking has become easy to do (see chart).

Cyber risk is notoriously difficult to quantify. Loss data are scarce and unreliable, in part because there is little incentive to report cyber losses, especially if the incident does not make headlines or there is no cyber insurance coverage. The rapidly evolving nature of the threats makes historical data less relevant in predicting future losses.

Scenario-based modeling, working out the costs of a well-defined incident affecting certain economies, produces estimates in the tens or hundreds of billions of dollars. Lloyd's of London estimates losses of $53.05 billion for a cloud service outage lasting 2½ to 3 days affecting the advanced economies. An IMF modeling exercise put the base-case average aggregated annual loss at $97 billion, with the worst-case scenario in the range of $250 billion.

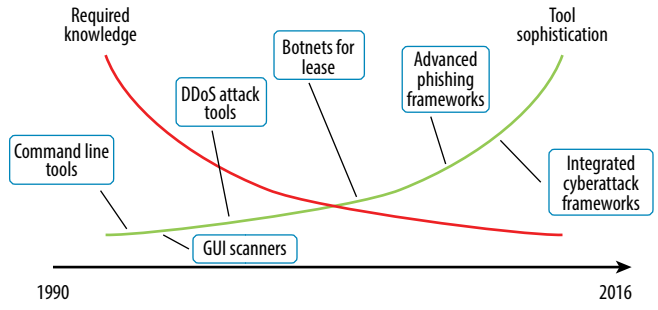
Causes and consequences

Crime in the physical world—with the intent of making money—is generally motivated simply by profit potentially much higher than for legal business, which criminals view as compensation for the high risk. In the world of cybercrime,

ART: ISTOCK/GURHAN YANREEL

Child's play

As tools become more sophisticated, hacking requires less technical knowledge, and it is now much easier to pull off a hack.



Source: Carnegie Mellon University.
Note: DDoS = distributed denial of service; GUI = graphical user interface.

similar or even higher profits are possible with much less risk: less chance of being caught and successfully prosecuted and almost no risk of being shot at. Phishing profitability is estimated in the high hundreds or even over a thousand percentage points. We can only speculate on the profits made possible by intellectual property theft carried out by the most sophisticated cyber threat actors. The basics, however, are similar: effective tooling and an exceptional risk/reward ratio make a compelling case and ultimately explain the sharp increase in and industrialization of cybercrime.

Cybercrime gives rise to systemic risk in several industries. While different industries are affected differently, the most exposed is probably the financial sector. A relatively new threat is posed by destruction-motivated attackers. When seeking to destabilize the financial system, they look at the most promising targets. Financial market infrastructure is the most vulnerable because of its pivotal role in global financial markets. Given the financial sector's dependence on a relatively small set of technical systems, knock-on effects from defaults or delays due to successful attacks can be widespread, with potentially systemic effects.

Given the inherent interconnection of financial sector participants, a successful disruption to the payment, clearing, or settlement systems—or stealing confidential information—would result in widespread spillovers and threaten financial stability.

Fortunately, to date, we have not experienced a cyberattack with systemic consequences. However, policymakers and financial regulators are increasingly wary, given recent incidents that took out ATM networks and attacks against online banking systems, central banks, and payment systems.

The financial sector has been dependent on information technology for decades and has a history of maintaining strong IT control environments mandated by regulation. While the financial sector may be most at risk of cyberattack, such attacks also carry a higher risk for cyber criminals, in part because of greater attention from law enforcement (just like old-fashioned bank robberies). The financial sector also does a better job of supporting law enforcement—for example, by keeping extensive records that are valuable in forensic investigations. Deeper budgets can often lead to effective cybersecurity solutions. (A recent notable exception is Equifax, whose hack was arguably a consequence of a cyber regulatory regime that was not proportional to its risk.)

The situation is different in health care. Except in the wealthiest nations, the health care sector typically does not have the resources necessary for effective cyber defense. This is evident, for example, in ransomware attacks this year that targeted computer systems at the electronic health record company Allscripts and two regional hospitals in the United States. Although also heavily regulated and under strict data protection rules, health care has not relied nearly as much on IT as the financial sector has, and consequently has not developed a similar culture of strict IT controls. This too makes the health care sector more susceptible to cyber breaches. What is most worrisome about this weakness is that, unlike in the financial sector, lives can be lost if, for example, attackers hit computerized life-support systems.

Utilities, especially the power and communication grids, are often cited as the next sectors where large-scale cyberattacks can have severe consequences. In this case, however, the main concern is

International cooperation in combating and prosecuting cybercrime lags well behind the global nature of the threat.

disruption or infiltration of systems by rival states, either directly or through proxy organizations. As famously exemplified by the massive 2007 attack against Estonia's Internet infrastructure—which took down online financial services, media, and government agencies—the more advanced and Internet-based an economy, the more devastating cyberattacks can be. Estonia is among the most digitalized societies in the world (see "E-stonia Takes Off" in the March 2018 *F&D*).

Countermeasures

If critical infrastructure—say, a power grid—or telecommunication and transportation networks are affected, or an attack prevents governments from collecting taxes or providing critical services, major disruptions with systemic economic implications could ensue and potentially pose a public health or security hazard. In such instances, the aggregate risk to the global economy could exceed the sum of individuals' risks, because of the global nature of IT networks and platforms, the national nature of response structures, ineffective international cooperation, or even the presence of nation-states among the attackers.

International cooperation in combating and prosecuting cybercrime lags well behind the global nature of the threat. The best way to tackle cybercrime is to attack its business model, which relies on the exceptional risk/reward ratio associated with ineffective prosecution. In this context, the business risk of cybercrime must be raised significantly, but this is possible only with better international cooperation.

Cybercrime operations can span several jurisdictions, which makes them harder to take down and prosecute. Some jurisdictions are slow, ineffective, or simply uncooperative in tackling cybercrime. Stronger cooperation would make tracking down suspects and charging them faster and more effective.

In the financial sector, regulators have developed specific assessment standards, set enforceable expectations and benchmarks, and encouraged information sharing and collaboration among firms and regulators. Bank regulators conduct IT examinations that factor cybersecurity preparedness into stress testing, resolution planning, and safety and soundness supervision. Some require simulated cyberattacks designed specifically for each firm, drawing on government and private sector intelligence and expertise, to determine resilience against an attack. Companies have also increased investment in cybersecurity and are incorporating cybersecurity preparedness into risk management. In addition, some have sought to transfer some risk via cyber insurance.

The current cybersecurity landscape remains disparate and decentralized, with risks handled mainly as local idiosyncratic problems. There are some cooperation mechanisms, and governments and regulators are stepping up their efforts, but the choice of cybersecurity is largely determined by corporate need—"each to its own." This must change to bring about generally enhanced cyber risk resilience. Strong preventive measures are needed both at the regulatory and technology levels and across industries. Among the most important of these is adherence to minimum cybersecurity standards, enforced in a coordinated way by regulators. Stepped-up cybersecurity awareness training will help defend against the basic technical weaknesses and user errors that are the source of most breaches.

Cyberattacks and cybersecurity breaches seem inevitable, so we also need to focus on how fast we detect breaches, how effectively we respond, and how soon we get operations back on track. FD

TAMAS GAIDOSCH, senior financial sector expert in the IMF's Monetary and Capital Markets Department, is a cybersecurity professional with more than 20 years' experience, including probing banking systems to find cyber weaknesses. He formerly led the Information Technology Supervision Department at the Central Bank of Hungary.