AUBURN UNIVERSITY
McCrary Institute

Policy Brief:
How the Economics of Cybersecurity Favor Attackers and What Defenders can do to Change the Dynamic

A report brought to you by
the McCrary Institute for Cyber and Critical Infrastructure Security
Auburn University

By

Kiran Sridhar, Senior Fellow
Frank Cilluffo, Director

Cyber attacks are wreaking havoc on American businesses. In 2023, the Internet Crime Complaint Center (IC3), an FBI-run clearinghouse, received reports of 850,000 crimes, leading to over $13 billion in losses.[1] As eye watering as that statistic is, IC3 acknowledges that many internet crimes are unreported, meaning the total cost of cybercrime is significantly higher. More troublingly, state-sponsored threat actors are burrowed into our critical infrastructure—the systems and services that are essential for society to function. For example, the Intelligence Community and technology firms have found that Volt Typhoon, a Chinese state-linked threat actor, has infiltrated communications, energy, transportation, and water systems and that another Beijing-backed threat group, Salt Typhoon, has hacked into telecommunications networks.[2] In the event of a future armed conflict, cyber attacks could be used by these actors to cripple our critical infrastructure, preventing or delaying the United States from mounting a response.[3]

Why have cyber threats remained so persistent? It is because the economics in cyberspace tend to favor the attackers. This is for two reasons. First, it's easy and cheap to perpetrate attacks. Our underlying technology infrastructure, including the systems of many critical infrastructure operators, is filled with vulnerabilities that attackers can cheaply exploit. Second, when attackers exploit these vulnerabilities, they are rarely punished, particularly relative to other crimes. In fact, while over 18% of property crimes and 46% of violent crimes are "cleared," meaning that the perpetrator is arrested and charged, less than 1% of cybercrimes were estimated to have been cleared in 2018.[4]

Cyber policymakers should focus on both hardening our cyber infrastructure, so that it is more expensive for cyber criminals to wage attacks, and on imposing costs on cyber criminals. We propose three strategies to achieve each of these two objectives.

Hardening America's Cyber Infrastructure

The Biden administration's 2022 National Cyber Strategy asserts that "market forces alone have not been enough to drive broad adoption of best practices in cybersecurity and resilience," implying that regulation may be necessary to drive better security posture. However, we must tread carefully whenever we feel compelled to fall back on an explicitly regulatory approach. Regulations sometimes can create the illusion that good cybersecurity is a mere compliance exercise. It is not. Adversaries are actively trying to elude any fence we erect. A gold-standard cybersecurity posture today may be insufficient tomorrow if attackers develop new exploitation techniques. Moreover, regulations may induce a torrent of lawsuits and increased compliance costs, making our innovative tech industry less dynamic, significantly diminishing growth potential.

Instead of a strictly regulatory approach, the government can correct market failures by eliminating information asymmetries and leveraging its purchasing power to create incentives. When regulations are promulgated, they must be carefully developed to avoid imposing excessive costs or having unintended consequences. The focus must be on outcomes and not just process. How should we expect the software and critical infrastructure we rely on to perform effectively during a cyber attack? By mandating performance standards instead of prescribing checklists, we will encourage the technology sector to cost-effectively deliver better security and reduce wasteful spending on unnecessary or ineffectual controls or security practices.

[1] *Internet Crime Report 2023*, Internet Crime Complaint Center, Federal Bureau of Investigation, U.S. Department of Justice, accessed November 25, 2024, <https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf>

[2] "PRC State-Sponsored Cyber Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024, *Cybersecurity Advisory*, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, accessed November 25, 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

[3] *Final Report of the U.S. Cyberspace Solarium Commission*, March 2020, accessed November 25, 2024, <https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view>.

[4] Eoyang, Mieke, Allison Peters, Brandon Gaskew, and Ishan Mehta, To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors," October 29, 2018, Third Way, accessed November 25, 2024, <https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors>.

Here are three steps the next administration should take:

1. Establish the National Cybersecurity Certification and Labeling Authority. ///

In 2004, legendary cryptologist Bruce Schneier identified a critical market failure in the procurement of technology products: information asymmetry. Purchasers of technology products lack the information to determine whether these products are secure. As a result, secure products don't command a price premium over insecure products, known as lemons. This creates what Nobel-laureate George Akerloff termed a "market for lemons." Technology producers have no incentives to invest in security and only lemons are sold. The market for lemons means that the technology products we rely on have inadequate security, not because manufacturers lack the ability to deliver secure products, but because they lack the motivation. Consequently, attackers have many potential vulnerabilities they can exploit to inflict damage.

The FCC has taken a partial step toward closing this information gap by introducing the Cyber Trust Mark certification program.[5] This initiative will certify the IoT devices that are developed in accordance with the voluntary NIST IoT cyber standards. Appliances that are judged to be compliant with these standards will receive a Cyber Trust Mark label, analogous to the DoE's Energy Star label that identifies energy efficient appliances. Purchasers will then know which products are secure, allowing these products to command a premium on the market.

Cyber Trust Mark is a great first step, as IoT devices are potent attack vectors for malicious cyber actors. But it doesn't go far enough. There are many other technology products that are insecure, and we need a more comprehensive certification regime to shift market incentives. In 2021, the congressionally mandated Cyberspace Solarium Commission proposed just that: a National Cybersecurity Certification and Labeling Authority.[6] This organization would be independently run by a nonprofit selected via a competitive bid process. It will receive funding from the government to develop cybersecurity standards and an accreditation process, in partnership with experts in academia, government, and the private sectors. The National Cybersecurity Certification and Labeling Authority will ensure that consumers are armed with the tools they need to make informed purchasing decisions.

2. Use government procurement to incentivize software manufacturers to prioritize cybersecurity. ///

In addition to information asymmetries, software manufacturers are disincentivized from adopting good security practices because they often bear no liability for security failures. Microsoft, for instance, says in its service level agreements that its customers are purchasing its software on an "as-is" basis, accepting "all faults," including any security vulnerabilities.[7] Since most software manufacturers bear none of the costs for security failures, and because secure products struggle to command a premium on the market, many software manufacturers have made the rational decision to give security short-shrift.

[5] "Fact Sheet: Cybersecurity Labeling for the Internet of Things," February 22, 2024, Federal Communications Commission, accessed November 25, 2024, <https://docs.fcc.gov/public/attachments/DOC-400674A1.pdf>

[6] *Final Report of the U.S. Cyberspace Solarium Commission*, March 2020, accessed November 25, 2024, <https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view>.

[7] "Version History Overview," October 3, 2024, Microsoft, accessed November 25, 2024, <https://learn.microsoft.com/en-us/SharePoint/version-overview>.

As the largest purchaser of software in the world, having spent $100 billion on IT, the federal government can correct this dynamic.[8] It purchases software from many of the largest companies in the world, so if the government impelled its software suppliers to invest more in security, all customers of the software—not just government agencies—would benefit.

In its service level agreements (SLAs) with software companies, the government can require that vendors fix vulnerabilities of specified severity within a certain time period or face financial penalties. With these SLAs, vendors would internalize the cost of poor cybersecurity and be motivated to ship out secure products. After all, it is far cheaper to fix a flaw during the code development stage than it is to remediate a vulnerability once a product has entered the market. By setting target outcomes instead of mandating specific practices, the government will allow software makers to identify and implement the security practices that provide the most bang-for-the-buck.

As Jeanette Manfra and Charley Snyder suggest, government procurement contracts should consider the security track record of software products, much as they already factor in a company's history of "on-time delivery, workmanship, and controlling cost."[9] Software manufacturers will not want to lose the potential of selling to the government, a highly lucrative customer. They will then invest more in cybersecurity than they do today.

3. Harden critical infrastructure by incentivizing operators to invest in capabilities that improve performance. ///

Most critical infrastructure is owned and operated by the private sector.[10] The operators and not the federal government are tasked with developing and implementing cybersecurity strategies to protect these critical assets. As General Keith Alexander, the first Commander of U.S. Cyber Command once noted, this means that critical infrastructure operators "are responsible for defending [themselves] in cyber space" against "nation-state attacks" that have the potential to cripple our society.[11] Making sure that critical infrastructure operators adopt strong cyber defenses is a security imperative.

Fortunately, the federal government still plays a critical role in incentivizing critical infrastructure operators to invest in cybersecurity. In the power sector, the Federal Electricity Regulatory Commission (FERC) sets the rates that utilities are allowed to charge. FERC can allow critical infrastructure operators to charge a fair premium for implementing robust cybersecurity programs. In other industries, such as the transportation and water sectors, the government disburses grants that help operators build and secure their technology infrastructure. The government thus has the leverage to compel critical infrastructure operators to adopt strong cybersecurity practices.

FERC took an admirable first step by implementing an "incentive-based rate" that allows for utilities to charge their customers more if they make "advanced cybersecurity investments."[12] However, it took an approach based, not on

[8] "Federal Software Licenses: Agencies Need to Take Action to Achieve Additional Savings," January 2024, Government Accountbility Office, accessed November 25, 2024, <https://www.gao.gov/assets/d24105717.pdf>

[9] Manfra, Jeanette and Charley Snyder, "CSRB Report Highlights the Need for New Approaches to Securing the Public Sector," May 20, 2024, *Google: The Keyword*, accessed November 25, 2024, <https://blog.google/technology/safety-security/csrb-report-google-recommendations/>.

[10] "Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing," March 1, 2022, Government Accountability Office, accessed November 25, 2024, <https://www.gao.gov/products/gao-22-104279>.

[11] Brunet, Jennifer S., General (Ret.) Keith B. Alexander (U.S. Army), Jamil N. Jaffer, "Clear Thinking about Protecting the Nation in the Cyber Domain," 2017, George Mason University, accessed November 25, 2024, <https://nationalsecurity.gmu.edu/wp-content/uploads/2017/03/CDRV2N1_Clear-Thinking_Alexander_Jaffer_Brunet_032217-1.pdf>.

[12] *Incentives for Advanced Cybersecurity Investment*, May 3, 2023, the Federal Energy Regulatory Commission, U.S. Department of Energy, accessed November 25, 2024, <https://www.federalregister.gov/documents/2023/05/03/2023-08929/incentives-for-advanced-cybersecurity-investment>.

cybersecurity performance, but on inputs. FERC listed a set of cybersecurity expenditures that were “pre-qualified” for this rate incentive, including the controls enumerated in the NIST Cybersecurity Framework.

This is a flawed approach. It hews to the view that good cybersecurity is a compliance exercise, which we believe not to be true. Promising new technologies come out frequently. Many of these technologies are not on the pre-qualified list. And as threats evolve, some controls that are not necessary today may be essential tomorrow. FERC’s rule inadvertently disincentivizes utilities from adopting these technologies.

Instead of prescribing the specific security tools that critical operators should adopt, the government should focus on outputs: how resilient critical infrastructure systems are to cyber attacks. The President’s Council of Advisors on Science and Technology suggested several “leading indicators of cyber-physical resilience.”[13] These indicators can be used to measure whether systems can withstand and recover from cyber attacks before attacks take place.

Government agencies like FERC could set targets based on these leading indicators. For example, it can judge operators based on how quickly they can rebuild a critical infrastructure system from scratch and what percentage of assets can pass “extreme offense, adversarial security” attack simulations. Companies should be given rate incentives or grants to meet these targets and only continue to receive these incentives if they meet prescribed benchmarks.

By leveraging these actions, our critical infrastructure systems will be able to repel and recover from the barrage of attacks they face.

Imposing costs on attackers

Hardening our cyber infrastructure will tilt the economics in cyberspace in defenders’ favor. However, cyber policymakers must remember a common adage in the security community: “Defenders must be right all the time. Attackers only must be right once.” Malicious actors often only need to find one point of weakness to infiltrate a target and achieve their objectives.

Thus, the deck is stacked against defenders, who are only human. They will inevitably slip up by forgetting to patch vulnerabilities, misconfiguring security tools, or clicking on dangerous links. The federal government should not blame victims. Instead, it should impose costs on adversaries. Our adversaries in cyberspace should think twice about waging attacks, even when they have clear attack vectors they can infiltrate.

To be sure, we lack the resources to identify and punish all cyber criminals or even all cyber criminals who target critical infrastructure. But by increasingly and more aggressively going after cyber criminals, we can deter cybercrime. Economists have found that when a city puts even one additional police officer on the streets, crime goes down.[14] Similarly, when the Justice Department and international partners took down LockBit, a leading cyber criminal organization, ransomware activity dropped by 30%, according to incident response firm Arctic Wolf’s research division.[15] Suddenly, criminals were concerned about getting caught and punished and they became far more circumspect.

[13] *Report to the President: Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World*, February 2024, President’s Council of Advisors on Science and Technology, Executive Office of the President, The White House, accessed November 25, 2024, < https://www.whitehouse.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf>.

[14] Chalfin, Aaron, Benjamin Hansen, Emily K. Weisburst, and Morgan C. Williams, Jr., “Police Force Size and Civilian Race,” June 2022, *American Economic Review*, Volume 4, Number 2, (pp. 139-158), <https://www.aeaweb.org/articles?id=10.1257/aeri.20200792>.

[15] Kruse, David, Reference to Arctic Wolf Labs Data, LinkedIn post, accessed <https://www.linkedin.com/posts/davidrkruse_cyberinsurance-cybersecurity-informationsecurity-activity-7208880059900727296-dE7M/?utm_source=share&utm_medium=member_desktop>.

Here are three additional steps law enforcement should take to build off the success of the LockBit takedown:

1. Disrupt the ransomware supply chain ///

Michael Daniel, former U.S. Cybersecurity Coordinator, notes that ransomware gangs have specialized a la Adam Smith. Some criminal groups focus on gaining initial access. Others focus on hosting phishing websites. Still others focus on developing malware that can encrypt attacked companies' systems. Multiple groups collaborate with each other to stage a single ransomware attack. While the ransomware supply chain has made criminal groups more potent, it also presents an opportunity for law enforcement agencies. By taking down critical and vulnerable nodes of the supply chain, the Department of Justice and its partners can cripple the entire ransomware ecosystem.

One place law enforcement should focus is on initial access brokers. Many ransomware criminals live in countries that do not have extradition treaties with the United States, making it nearly impossible to arrest them. But increasingly, initial access brokers are U.S.-based or in other English-speaking countries. Consider Scattered Spider, a group of US- and UK-based teenagers and twenty-somethings behind the attacks on MGM and Caesar's Palace. Scattered Spider was able to gain initial access in large part because its members were fluent English speakers. They can call help desks, impersonate employees, claim to have lost login credentials, and dupe IT staff into giving them new login credentials. Scattered Spider has been so effective that other initial access brokers are emulating them. But western-based cyber criminals can more easily be identified and arrested, as Scattered Spider members and their copycats should be. Police in Spain took the right first step by arresting a Scattered Spider leader, a measure other law enforcement groups should emulate.[16]

Second, law enforcement should target ransomware service providers. These entities can sometimes serve hundreds of ransomware gangs—meaning a single takedown can waylay many criminals. Consider the April 2024 takedown of LabHost, a phishing as a service provider. LabHost created phishing templates for ransomware criminals, who could stand up fake Spotify, DHL, or JP Morgan pages designed to steal user credentials. By taking LabHost down, the FBI removed 40,000 fraudulent sites used by 2,000 criminals and in its 2023 dismantling of LolekHosted, a "bulletproof" hosting service used by hundreds of botnets, ransomware gangs, and DDoS attackers, EUROPOL was able to seize 300 terabytes of data, crucial intelligence which it is now using to catch other cyber criminals. To be sure, new services will emerge to fill the void left by LabHost and LolekHosted. But these takedowns will slow criminals down, giving a much-needed reprieve to overwhelmed security teams. If this sort of deterrence were more common, opportunistic criminals would be more hesitant to offer similar services, because they know they would be targets of law enforcement.

Third, and most importantly, federal investigators should home in on the ransomware service providers that add the most value. Some ransomware suppliers offer commoditized services that can easily be replaced. Others offer critical—and hard to replicate—services. The makers of ransomware encryption software are furthest up the value chain because it is difficult to "encrypt victims' systems without using so much CPU power as to give the game away," notes journalist Alexander Martin. The FBI, in concert with its foreign partners, should focus significant resources on arresting or incapacitating the most valued members of the cybercrime ecosystem, including encryption software manufacturers.

2. Adopt "hot spot policing" to better protect critical infrastructure ///

Not all targets of cybercrime are equal. Society faces severe consequences when critical infrastructure systems are hit by cyber attacks. When Colonial Pipeline suffered a ransomware attack, for instance, it caused fuel prices to rise to their

[16] "Alleged Boss of 'Scattered Spider' Cyber Hacking Group Arrested," June 15, 2024, *Krebs on Security*, accessed November 25, 2024, <https://krebsonsecurity.com/2024/06/alleged-boss-of-scattered-spider-hacking-group-arrested/>.

highest level in seven years.[17] And when hospitals are hit by ransomware attacks, it causes the mortality rate for their Medicare patients to increase by one-third, according to a working paper from University of Minnesota economists.[18]

We must deter cyber criminals from targeting critical infrastructure. We should borrow a page from big-city law enforcement playbooks and adopt "hot spot policing," an approach pioneered in the 1990s, when New York City was beset by violent crime. Police commissioner Bill Bratton used innovative CompStat software to pinpoint the neighborhoods and blocks where the most serious violent crimes were taking place. He then "blanketed [these areas] with uniformed and plainclothes" officers who would conduct regular surveillance and arrests.[19] Through this approach, the NYPD interdicted criminals before they could commit serious crimes. The result: shootings in New York City fell from 1,700 in 1998 to less than 800 in 2018.[20]

Cyber law enforcement officers should similarly increase their surveillance of the dark web forums where malicious access to hospitals and other critical infrastructure operators is sold. They should identify both the sellers and buyers in these forums. And they should do everything in their power to stop these actors from committing crimes. If possible, they should be arrested. If not, their IT systems should be bricked through offensive operations. And when these criminals do perpetrate successful attacks on critical infrastructure systems, law enforcement should seize their ill-gotten gains.

Hot spot policing is not a panacea. Cyber criminals may shift their efforts to other industries where they are less likely to incur the wrath of law enforcement. But hot spot policing should markedly reduce the cyber attacks that are most costly to society: those that target critical infrastructure operators.

3. List the state sponsors of cyber crime and designate transnational cyber criminal organizations ///

Even if law enforcement authorities can pinpoint more cyber criminals, they will struggle to arrest them. That is because rogue nations provide safe haven to cyber criminals. Russia, for instance, allows ransomware gangs to operate with impunity, if they do not target Russian companies and occasionally conduct operations at the behest of the Kremlin's intelligence services. Because of Russia's permissive stance, Russian-speaking ransomware gangs captured almost 70% of total ransomware proceeds in 2023. Much as the US government has fought to eliminate terrorist safe havens, it should work to eliminate cyber crime safe havens.

The State Department should borrow a successful page from its War on Terror playbook by introducing a list of state sponsors of cyber crime. A state could be listed as a state sponsor of cyber crime if it actively abets a criminal group; profits from cyber crime; or interferes with US or ally investigations into cyber crime. Creating this list will enable the US government to impose sanctions and diplomatic penalties, such as restricting foreign aid. It would be a powerful inducement for countries to get serious about combatting cyber crime within their borders.

[17] "Panic Buying Strikes Southeastern United States as Shuttered Pipeline Resumes Operation," May 12, 2021, *The Washington Post*, accessed November 25, 2024, <https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/>.

[18] McGlave, Claire C., Hannah Neprash, Sayeh Nikpay, *Hacked to Pieces? The Effect of Ransomware Attacks on Hospitals and Patients*, October 4, 2023, University of Minnesota Twin Cities School of Public Health, accessed November 25, 2024, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292>.

[19] *Measuring What Matters: Proceedings from the Policing Research Institute Meetings*, July 1999, National Institute of Justice, Office of Community Oriented Policing Services, Office of Justice Programs, U.S. Department of Justice, accessed November 25, 2024, <https://www.ojp.gov/pdffiles1/Digitization/179856-179864NCJRS.pdf>.

[20] Bratton, William, "Police Reform Needs to Come from Within," *The Atlantic*, July 22, 2022, accessed November 25, 2024, <https://www.theatlantic.com/ideas/archive/2022/07/police-reform-violent-crime-wave-new-york/670497/>.

The Treasury Department can also designate multiheaded cyber criminal groups as transnational criminal organizations (TCOs). US citizens and institutions are proscribed from transacting with TCOs—significantly hindering them from proceeding with operations.

Collectively, these steps will make it more expensive for attackers to exploit vulnerabilities and will punish and deter cyber criminals. This will level the playing field between defenders and attackers.