Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

TRADE SECRET PROTECTION IN THE DIGITAL ERA: CYBERSECURITY THREATS AND LEGAL REMEDIES

Navruzbek Tilaboev
University of Illinois at Urbana-Champaign Law College
nova.tilaboyev@gmail.com

Abstract
Corporate espionage did not disappear in the digital age. It got cheaper, faster, and dramatically harder to detect. Today, a trade secret that once required a mole inside a company or a briefcase full of stolen documents can be exfiltrated by a skilled adversary in minutes, from the other side of the world, without ever triggering an alarm. This article examines the growing mismatch between the legal architecture designed to protect trade secrets and the cybersecurity realities companies now face. It surveys the primary threat vectors — from nation-state intrusions and ransomware to insider threats and supply chain compromises — and evaluates the legal remedies available under the Defend Trade Secrets Act, state law, and international frameworks. The analysis is candid about the limits of litigation as a response to cyber-enabled misappropriation and proposes a more integrated approach that treats legal and technical protections as inseparable rather than sequential.

Keywords: Trade secrets; cybersecurity; digital espionage; Defend Trade Secrets Act; data breach; insider threat; misappropriation; nation-state attacks; legal remedies; reasonable measures; supply chain security; incident response

I. Introduction

In 2014, the United States Department of Justice indicted five members of the Chinese People's Liberation Army for hacking into the computer systems of American companies including Westinghouse Electric and U.S. Steel, stealing technical specifications, pricing strategies, and negotiating positions that China's

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

state-owned enterprises then used against those same American firms at the bargaining table.[1] It was, for many legal practitioners, a clarifying moment. The threat was not hypothetical. The damage was not speculative. And the law, for all its sophistication, had almost nothing to offer the victims in any practical sense. The defendants were military officers operating from a foreign country. No extradition was coming. The indictments were, in the words of one observer, "a well-dressed press release." That episode captures something important about the challenge of protecting trade secrets in a networked world. The legal frameworks we rely on — the Defend Trade Secrets Act, the Economic Espionage Act, state trade secret statutes — are not without value. They provide real remedies in cases involving domestic actors, disgruntled former employees, and competitors who operate within reach of U.S. courts. But the most sophisticated and most damaging threats increasingly originate from actors who are beyond those courts' practical jurisdiction, who leave little forensic evidence, and who can accomplish in a single intrusion what physical theft would have required years to achieve.

None of this means the law is useless. It means the law has to be understood for what it is: one layer of protection among several, and not always the most important one. Companies that treat trade secret protection as primarily a legal problem, to be handled by counsel when something goes wrong, are misunderstanding the nature of the risk they face. The companies that manage this risk most effectively are the ones that have integrated legal strategy with cybersecurity infrastructure, so that the two reinforce each other rather than operating in parallel universes.[2]

This article tries to bridge that gap. Part II provides a working overview of the legal framework for trade secret protection, with attention to the features that matter most in cyber-theft scenarios. Part III maps the principal cybersecurity threat vectors and examines how each one interacts with existing legal doctrine. Part IV surveys available legal remedies and assesses their practical effectiveness. Part V addresses the internal governance structures that make the difference between companies that successfully assert trade secret claims and those that cannot. Part VI offers a frank assessment of where the current approach falls short and what a more adequate response might look like.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

II. The Legal Architecture: What We Have to Work With

A. The Defend Trade Secrets Act

When Congress passed the Defend Trade Secrets Act in 2016, it did so with cyber-enabled misappropriation squarely in mind. The legislative history makes clear that members were concerned not only with the traditional insider-theft scenario but with the growing reality of foreign and domestic cyber intrusions targeting American commercial secrets.[3] The result was a statute broad enough to cover digital theft while grounded in doctrinal concepts developed over decades of state law experience.

The DTSA's definition of a trade secret is intentionally expansive: any form of financial, business, scientific, technical, economic, or engineering information that derives independent economic value from its secrecy and that the owner has taken reasonable measures to keep secret.[4] That last phrase — reasonable measures — is where things get interesting in the cybersecurity context. Courts have consistently held that the "reasonable measures" inquiry is fact-specific and context-dependent, which means a company's cybersecurity posture becomes directly relevant to whether it can successfully assert a trade secret claim after a breach. We will return to this.

The Act provides for injunctive relief, compensatory damages, and, in cases of willful and malicious misappropriation, exemplary damages up to twice the compensatory amount together with attorney's fees.[5] In egregious cases, ex parte civil seizure orders are available, though courts grant these sparingly. The criminal counterpart, the Economic Espionage Act of 1996, provides for prosecution of foreign-government-sponsored theft as well as domestic commercial espionage, with penalties of up to fifteen years imprisonment and fines up to five million dollars.[6]

B. State Law: Still Relevant

The DTSA preserved state trade secret claims rather than preempting them, and for good reason. State law remedies, particularly under variants of the Uniform Trade Secrets Act, often provide procedural advantages or damages frameworks that complement federal claims. Forty-eight states and the District of Columbia

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

have adopted some version of the UTSA, though the details vary enough that choice of law analysis remains important in multistate disputes.[7]

State courts also bring familiarity with local business communities and, in some jurisdictions, specialized commercial divisions with genuine expertise in trade secret matters. For purely domestic disputes, state law can be the more efficient vehicle. The practical reality for most cyber-enabled misappropriation cases, however, is that the DTSA's federal forum and nationwide service of process make it the preferred starting point.

C. International Frameworks and Their Limits

The international dimension of trade secret protection is, to put it diplomatically, underdeveloped. TRIPS requires WTO member states to protect undisclosed information meeting the basic criteria of secrecy, commercial value, and reasonable protective efforts.[8] The EU's Trade Secrets Directive (2016/943/EU) brought meaningful harmonization within Europe.[9] Bilateral and multilateral trade agreements increasingly include trade secret provisions with at least nominal enforcement mechanisms.

In practice, none of this helps much when the defendant is a state-sponsored hacking unit or a company operating under the protection of a government that has decided it prefers industrial espionage to trade. The gap between the nominal international framework and the enforcement reality is wide enough to drive a server farm through. Companies operating internationally need to understand that legal protection, in many jurisdictions, amounts to a right without a practical remedy. That understanding should shape their security investments accordingly.

III. The Cybersecurity Threat Landscape

A. Nation-State Actors

The most capable and most damaging threat to corporate trade secrets comes from nation-state actors, primarily but not exclusively from China, Russia, Iran, and North Korea. What distinguishes these adversaries from ordinary cybercriminals is not just their technical sophistication, though that is often formidable. It is their patience, their resources, and their specific targeting. They

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

are not casting wide nets looking for credit card numbers. They are pursuing defined objectives: the formula for a pharmaceutical compound, the specifications for a semiconductor fabrication process, the pricing models of a defense contractor.[10]

The FBI's Cyber Division has described the threat from Chinese state-sponsored actors as the most significant long-term counterintelligence threat facing the United States, and there is no reason to think that assessment is overstated.[11] Operation Cloud Hopper, attributed to the Chinese group APT10, targeted managed service providers as a vector for accessing client networks across dozens of countries, a supply chain attack that demonstrated a level of strategic sophistication that most corporate legal departments were simply not prepared to address. The legal frameworks available to victims were, in most cases, wholly inadequate to the actual harm suffered.

B. Ransomware and Double Extortion

Ransomware has evolved into something more legally complex than it first appeared. In the early days, it was relatively straightforward: malicious software encrypted a victim's files, the attacker demanded payment for the decryption key, and the trade secret concern was primarily about operational disruption rather than information theft. That model has been largely superseded by what practitioners now call double extortion.

In double extortion attacks, the attacker exfiltrates data before encrypting it and threatens to publish or sell that data if the ransom is not paid.[12] From a trade secret perspective, this creates a genuine disclosure risk, not a theoretical one. Groups like LockBit and ALPHV operated dedicated leak sites where they published stolen corporate data from victims who refused to pay or pay quickly enough. Whether that publication constitutes misappropriation under the DTSA is a question courts have only recently begun to confront, and the answers are not yet settled.

The legal complexity deepens when you consider the victim's position. Paying the ransom may prevent publication, but it raises potential issues under OFAC sanctions regulations if the ransomware group has been designated a sanctioned entity. Not paying may result in disclosure of trade secrets. Neither option is

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

clean, and the legal guidance available to companies facing these decisions in real time remains inadequate to the actual dilemmas involved.

C. The Insider Threat

Nation-state hackers attract the headlines, but insiders remain responsible for a substantial share of trade secret misappropriation. The Verizon Data Breach Investigations Report has consistently found that a significant proportion of data theft incidents involve current or former employees, contractors, or business partners with legitimate access.[13] The digital environment has made insider theft dramatically easier: a departing employee who once would have needed to photocopy documents now walks out with a thumb drive or, more likely, uploads files to a personal cloud storage account using the same Wi-Fi connection their employer provides.

What has changed in recent years is the scale and targeting of insider theft. The cases that end up in litigation increasingly involve employees who spent months or years systematically gathering proprietary information in anticipation of joining a competitor or launching a competing enterprise. The Waymo v. Uber litigation, discussed in the prior article in this series, is perhaps the most prominent example, but there are hundreds of less famous cases working through courts at any given moment.

Detection is the central challenge. Behavioral analytics tools can identify anomalous data access patterns, and data loss prevention software can flag unusual transfers. But these tools generate noise as well as signal, and in organizations where employees routinely move large files as part of legitimate work, the signal is hard to distinguish. By the time an insider theft is discovered — often only after the employee has departed and joined a competitor — the damage is done and the evidence is wherever the employee chose to put it.

D. Supply Chain Vulnerabilities

The SolarWinds intrusion of 2020, in which attackers compromised a widely used network management platform and used it to access the systems of thousands of downstream customers including multiple U.S. government agencies, demonstrated in the starkest possible terms the risk that third-party

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

vendors represent to a company's most sensitive information.[14] For trade secret purposes, the implication is significant: a company's protective measures are only as strong as those of its least secure vendor with access to its systems or data.

This creates a real problem for the "reasonable measures" analysis under the DTSA. A company can have world-class internal cybersecurity and still suffer a devastating intrusion through a compromised vendor. Whether courts will hold that a failure to adequately vet third-party security constitutes an unreasonable failure to protect trade secrets is still being worked out in litigation. The early indications suggest that courts expect companies to have vendor security programs, but the specificity of what is required remains unclear.

IV. Legal Remedies: What Works, What Does Not

A. Civil Litigation Under the DTSA

For domestic defendants within the reach of U.S. courts, civil litigation under the DTSA offers real remedies. Injunctive relief can prevent ongoing use of misappropriated information and, in appropriate cases, can restrict a departed employee from working in certain roles for a defined period. Damages can be substantial: in cases involving willful misappropriation, the combination of actual damages, unjust enrichment, and exemplary damages can reach figures that genuinely hurt even large defendants.

The practical challenges are significant, though. Trade secret litigation is expensive and slow. The discovery process in cases involving sophisticated digital intrusions requires forensic experts, extended timelines, and substantial cost. The burden of proving that specific information qualifies as a trade secret, that the plaintiff took reasonable measures to protect it, and that the defendant misappropriated it through improper means — all while the defendant denies everything and challenges every element — is real and should not be underestimated.[15]

Attribution is often the hardest problem. In a cyber intrusion case, establishing that the defendant was responsible for the intrusion, not just the beneficiary of stolen information, requires technical evidence that may be difficult to obtain through civil discovery. Courts have shown some flexibility in allowing

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

plaintiffs to rely on circumstantial evidence of access and use, but defendants with sophisticated legal counsel will challenge attribution aggressively.

B. Criminal Prosecution

The Economic Espionage Act provides federal criminal jurisdiction over both foreign government-sponsored trade secret theft and domestic commercial espionage.[16] Prosecutions under the EEA have increased meaningfully since 2016, reflecting both the growing scale of the problem and an increased commitment of federal enforcement resources. The Department of Justice's China Initiative, though its formal structure has been modified, represented a sustained effort to prioritize prosecution of state-sponsored economic espionage. The limits of criminal prosecution in this context are obvious but worth stating. Criminal cases require the defendant to be within the jurisdiction. Against foreign state actors operating from countries with no extradition treaties, indictments serve primarily as public statements of attribution and deterrence rather than practical enforcement tools. The 2014 PLA indictments mentioned in the introduction produced no arrests. Neither have most subsequent indictments of foreign nationals for cyber-enabled trade secret theft. This is not a criticism of the prosecutors involved; it is a structural reality that companies need to understand when calibrating their expectations.

C. Emergency Relief and Provisional Remedies

In cases where misappropriation is discovered quickly, emergency injunctive relief can be the most valuable legal tool available. Temporary restraining orders and preliminary injunctions can prevent a departing employee from using stolen information, stop a competitor from launching a product based on misappropriated technology, or freeze assets pending resolution of the underlying claim.[17]

The DTSA's ex parte seizure provision, while rarely used, deserves mention. In genuine emergencies, where there is reason to believe that a defendant would destroy or conceal evidence if given notice, courts have the authority to order seizure of the misappropriated property without advance notice to the defendant. The bar for this remedy is appropriately high, but practitioners should be aware

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

of it. Speed matters enormously in trade secret cases, and counsel who understand the full toolkit available can make a real difference in outcomes.

D. International Options

For companies operating internationally, the picture is patchy. EU member states offer reasonably robust civil remedies under their implementations of the Trade Secrets Directive. The UK maintains strong trade secret protections post-Brexit. Several Asian jurisdictions, including Japan and South Korea, have strengthened their trade secret regimes significantly in response to concerns about industrial espionage. But in many jurisdictions where sophisticated cyber intrusions originate, the nominal legal framework is irrelevant because there is no realistic prospect of enforcement.[18]

Diplomatic channels and trade agreement mechanisms have produced some results at the margins — the 2015 Obama-Xi agreement on commercial cyber espionage, for instance, was followed by a documented decline in Chinese state-sponsored intrusions targeting U.S. commercial entities, at least temporarily. But these mechanisms operate on long timescales and with uncertain outcomes. They are not a substitute for robust technical and legal protections at the company level.

V. Getting the Internal Architecture Right

A. The "Reasonable Measures" Standard as a Governance Framework

Here is a point that does not get enough attention in legal discussions of trade secret protection: the "reasonable measures" requirement in the DTSA and the UTSA is not just a legal threshold to clear in litigation. It is, properly understood, a governance framework. When a court asks whether a company took reasonable measures to protect its trade secrets, it is asking a question about how the company was actually run, not just about what its policies said on paper.

Companies that invest in cybersecurity infrastructure, conduct regular risk assessments, maintain access controls calibrated to information sensitivity, train employees on confidentiality obligations, and monitor for anomalous behavior are not just building a litigation defense. They are operating the way a well-managed organization should operate. The legal standard and good management

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

practice point in the same direction. The problem is that too many companies treat them as separate concerns, with legal counsel handling the policy documents and IT handling the technical infrastructure, and nobody ensuring the two are actually aligned.[19]

B. Information Classification and Access Control

The foundation of any serious trade secret protection program is knowing what you are trying to protect. That sounds obvious. It is routinely neglected. Many organizations have vast amounts of potentially proprietary information scattered across systems, shared drives, email archives, and collaboration platforms, with no systematic effort to identify which of that information actually constitutes trade secrets, where it lives, and who has access to it.

Without that mapping exercise, neither the legal team nor the security team can do their jobs effectively. You cannot protect what you have not identified. You cannot detect a breach of information you have not catalogued. You cannot assert trade secret rights in litigation over information that, upon examination, turns out to have been accessible to half the organization without restriction. Information classification is unglamorous work. It is also foundational, and the organizations that skip it are building everything else on sand.[20]

C. Incident Response Planning

When a cybersecurity incident occurs — and for companies holding valuable trade secrets, the question is when, not if — the first hours and days are critical for both security and legal purposes. Evidence preservation, forensic investigation, notification decisions, and litigation holds all need to happen quickly and in a coordinated way. Organizations that have thought through these processes in advance are in a fundamentally different position than those improvising under pressure.

Incident response planning should involve legal counsel from the start, not as an afterthought. Decisions made in the immediate aftermath of a breach, about what to preserve, what to disclose, how to communicate with employees and vendors, and whether to engage law enforcement, have legal consequences that are difficult to undo. Attorney-client privilege and work product protections need to

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

be established carefully to protect the investigation. Outside counsel should be identified before an incident, not during one.

D. Employee Lifecycle Management

A disproportionate share of trade secret litigation arises from employee departures. Hiring someone away from a competitor, or losing a key employee to one, is a routine feature of competitive markets. It becomes a legal dispute when the employee carries proprietary information with them. Managing this risk requires attention at multiple points in the employment relationship: clear confidentiality agreements at hiring, periodic reminders during employment, structured offboarding processes that include return of materials and device review, and exit interviews that address confidentiality obligations specifically.[21]

On the hiring side, companies need to be thoughtful about what they ask new employees to bring from their former employers. The risks run in both directions: the employee who voluntarily brings a competitor's trade secrets creates exposure for the new employer, not just the old one. Counsel advising on competitive hiring situations should be alert to these risks and build appropriate safeguards into the onboarding process.

VI. An Honest Assessment: Where the Current Approach Falls Short

Let me be direct about something the legal literature often hedges around. The current framework for trade secret protection in the digital era is, for many of the most serious threats, not working. Not because the statutes are badly drafted or the courts are incompetent. It is not working because the most damaging actors — nation-state hackers, organized criminal groups operating from non-cooperative jurisdictions, sophisticated insiders who plan their thefts carefully and cover their tracks — are largely beyond the practical reach of the legal system.

This is not an argument for giving up on legal protections. It is an argument for honest prioritization. The DTSA is valuable against domestic competitors who steal through employees or intrusions that can be traced to actors within U.S. jurisdiction. Criminal prosecution deters some domestic actors and, at least

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

symbolically, names and shames foreign ones. Civil litigation creates real consequences for companies and individuals who can be sued in U.S. courts. These are not trivial benefits.

But the companies most at risk from the most capable threat actors, technology companies holding cutting-edge intellectual property, defense contractors, pharmaceutical firms with valuable drug development pipelines, financial institutions with proprietary trading algorithms, need to approach trade secret protection primarily as a security problem and secondarily as a legal one. The legal framework is a backstop, a tool for accountability and remediation when something goes wrong. It is not, and cannot be, the primary line of defense against adversaries who operate in places where U.S. courts have no reach.[22]

What would a more adequate framework look like? At the domestic level, the DTSA could be strengthened with more specific provisions addressing cyber-enabled misappropriation, clearer standards for the "reasonable measures" analysis in digital contexts, and expanded provisions for evidence preservation orders in the early stages of litigation. At the international level, the development of meaningful mutual legal assistance frameworks with key trading partners, combined with credible consequences for state-sponsored espionage through trade policy mechanisms, would help close the enforcement gap that makes foreign-actor cases so frustrating.

At the company level, the answer is integration. Legal counsel, cybersecurity teams, and senior leadership need to treat trade secret protection as a shared responsibility with a shared strategy, not as separate functions that interact only when a crisis forces them together. The threat has integrated itself. The response needs to do the same.

References

1. United States v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu & Gu Chunhui, Indictment, No. 14-cr-00118 (W.D. Pa. May 1, 2014). See also U.S. Department of Justice, Attorney General Holder Speaks at the Press Conference on Charges Against Five Members of Chinese Military Unit (May 19, 2014).

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

2. Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux. See also National Counterintelligence and Security Center. (2023). Annual Report on Foreign Economic Collection and Industrial Espionage. Office of the Director of National Intelligence.
3. S. Rep. No. 114-220, at 2–4 (2016) (Senate Judiciary Committee Report on the Defend Trade Secrets Act of 2016).
4. 18 U.S.C. § 1839(3) (2016).
5. 18 U.S.C. § 1836(b)(3) (2016).
6. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831–1839).
7. National Conference of Commissioners on Uniform State Laws. (1985). Uniform Trade Secrets Act with 1985 Amendments.
8. Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.
9. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets), 2016 O.J. (L 157) 1.
10. Mandiant. (2023). M-Trends 2023: Special Report. Mandiant Threat Intelligence. https://www.mandiant.com/m-trends
11. Federal Bureau of Investigation. (2022). FBI Director Wray's Remarks at the Reagan Presidential Library: Countering the Chinese Government's Economic Espionage. https://www.fbi.gov/news/speeches
12. Coveware. (2023). Ransomware Attackers Down But Not Out After Disruptions. Quarterly Ransomware Report, Q4 2023. https://www.coveware.com/ransomware-quarterly-report
13. Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/
14. Cybersecurity and Infrastructure Security Agency. (2021). Alert (AA21-008A): Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/cybersecurity-advisories

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 3, March, 2026
Website: usajournals.org

15. Almeling, D. S., Snyder, D. W., Sapoznikow, M., McCollum, W. E., & Weader, J. (2010). A Statistical Analysis of Trade Secret Litigation in Federal Courts. Gonzaga Law Review, 45(2), 291–334.
16. 18 U.S.C. § 1831 (2016) (Foreign Economic Espionage); 18 U.S.C. § 1832 (2016) (Theft of Trade Secrets).
17. Quinto, D., & Singer, S. H. (2012). Trade Secrets: Law and Practice. Oxford University Press. See also updated analysis in Almeling, D. S. (2023). Trade Secret Law in the Age of Cyber Theft. Hastings Law Journal, 74(3), 601–655.
18. WIPO. (2020). Trade Secrets and the Digital Economy. World Intellectual Property Organization Publication No. 961E. https://www.wipo.int/publications/en/details.jsp?id=4476
19. Pooley, J. (2022). Trade Secrets: The Use of Confidential Business Information and Know-How in Commerce (2nd ed.). Law Journal Press. See especially Chapter 4 on reasonable measures.
20. Levine, J. S., & Sandeen, S. K. (2015). Cases and Materials on Trade Secret Law. West Academic Publishing.
21. Lobel, O. (2013). Talent Wants to Be Free: Why We Should Learn to Love Leaks, Raids, and Free Riding. Yale University Press.
22. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018