Using cyberweapons to steal trade secrets

by Vasilis Katos, Kenneth Wright
and John Zacharia

Introduction

Trade secrets are among the most valuable forms of intellectual property. Increasingly, like other valuable proprietary information, trade secrets are stored in digital form. As with any information stored digitally, trade secrets are vulnerable to cyberattacks. This article explores the definition of trade secrets, examines the cyberweapons online criminals use to exfiltrate digital information, and discusses how such cyberweapons may be used to steal trade secrets.

Trade secrets

Description of trade secrets

In today's knowledge-driven economy, the value of information can easily eclipse that of physical assets. Among the most critical yet least visible forms of intellectual property (IP) are trade secrets, confidential business information that offers companies a strategic advantage precisely because it remains undisclosed to competitors.

Trade secrets span a wide variety of proprietary knowledge, ranging from customer databases and pricing strategies to complex algorithms and chemical formulas. To qualify as a trade secret, information must meet three core criteria. First, it must be secret, meaning it is not generally known or readily accessible to people who typically deal with such information (competitors). Second, it must have commercial value to competitors. And third, the business must take reasonable steps to safeguard its confidentiality, such as implementing non-disclosure agreements, limiting physical or digital access, and training employees on information-security practices.

> **As businesses continue to operate in an environment of rapid innovation and high employee mobility, the strategic management of trade secrets is becoming as essential as protecting patents or trademarks.**

The legal frameworks governing trade secrets vary globally but share foundational principles. In the United States, trade secrets are protected under both State (mostly based on the Uniform Trade Secrets Act (UTSA) and Federal law pursuant to the Economic Espionage Act (EEA). The EEA defines trade secrets broadly as all forms of tangible or intangible information that derive economic value from not being generally known to competitors and are subject to reasonable confidentiality measures.

The European Union (EU) introduced a harmonised approach with the EU Trade Secrets Directive (Directive (EU) 2016/943). This legislation aligns Member

States around a common definition, stating that a trade secret is information that is secret, has commercial value due to its secrecy, and has been reasonably protected by its holder. The Directive aims to balance business protection with transparency and the mobility of workers.

Unlike patents, trade secrets can offer potentially indefinite protection, but only as long as the information remains confidential. The risk, however, is that once exposed, a trade secret loses its legal shield. Misappropriation – acquiring or using trade secrets through improper means such as theft, bribery, or breach of contract – can lead to significant civil and, in some cases, criminal liability. Civil remedies typically include injunctions, damages, and in urgent cases, seizure of stolen materials under court order. Criminal remedies include imprisonment.

"In today's knowledge-driven economy, the value of information can easily eclipse that of physical assets. Among the most critical yet least visible forms of intellectual property (IP) are trade secrets

As businesses continue to operate in an environment of rapid innovation and high employee mobility, the strategic management of trade secrets is becoming as essential as protecting patents or trademarks. Organizations that systematically identify, secure, and monitor their proprietary information stand to benefit not only from legal safeguards but from

a sustainable competitive edge – one that remains out of sight, but very much in force.

Description of types of trade secrets that are typically stored in digital form on a server (e.g., prototype design of a new semiconductor chip, pre-release music/movie/ fashion design)

As innovation moves increasingly into digital environments, trade secrets, once only locked in filing cabinets, are now stored on servers and cloud platforms. These high-value assets span industries and are central to competitive advantage, yet they are also highly vulnerable to cyber threats and internal leaks.

In the technology and manufacturing sectors, prototype designs such as digital files for semiconductor chips or consumer electronics are prime targets. Their exposure can erode competitive positioning and disrupt product roadmaps. Similarly, pre-release content in media – like unreleased films, music, or video games – is closely guarded to prevent leaks that could damage revenue or marketing strategies.

Source code, proprietary algorithms, and training data are the crown jewels of software and artificial intelligence (AI) firms. Stored in private repositories, they represent years of research and development and are often at the core of a company's IP portfolio. In the life sciences and chemicals industries, digital product formulations and test data are essential trade secrets, carefully managed through secured data environments.

Even creative sectors such as fashion and architecture rely on digital protection for pre-release designs and campaign assets, which can be compromised long before public launch. Alongside these are internal strategic documents – pricing models, product roadmaps, or market entry plans – which, if exposed, can undermine competitive moves.

As more of these assets are stored and exchanged in digital form, robust cybersecurity, access control, and a strong culture of confidentiality are essential. In an age where information moves fast and threats evolve rapidly, safeguarding digital trade secrets is no longer optional – it is foundational.

Economic impact if trade secrets are stolen

Trade secrets are often the invisible backbone of a company's competitive edge. When these secrets are stolen, the economic fallout can be devastating, not just for individual businesses but for entire industries and economies.

At the corporate level, theft of trade secrets can rapidly erode a company's market position. Competitors armed with proprietary formulas, designs, or strategies can flood the market with knockoffs or improved products at lower prices, undercutting the original innovator. This leads to lost sales, declining profits, and in some cases, irreversible brand damage. The financial blow does not stop there - companies face substantial costs related to legal battles, cybersecurity upgrades, and crisis management efforts to mitigate the damage.

Investor confidence can also take a hit when sensitive information is compromised. A breach signals potential vulnerabilities in management and governance, often triggering stock price drops and reduced capital inflows. In fast-paced industries like technology or pharmaceuticals, where first-mover advantage is critical, losing trade secrets can translate into lost opportunities worth millions or even billions of dollars.

On a broader scale, the theft of trade secrets poses a significant threat to national economies. Cyber-espionage campaigns targeting proprietary innovations disrupt innovation cycles and discourage research and development investments. This erosion of intellectual property protection undermines the very incentives that fuel economic growth and technological advancement. Furthermore, it can lead to job losses as companies scale back or relocate operations to safer jurisdictions.

“ As innovation moves increasingly into digital environments, trade secrets, once only locked in filing cabinets, are now stored on servers and cloud platforms

Governments and industry leaders increasingly recognise that safeguarding trade secrets is essential not only for individual business success but for maintaining global economic competitiveness. The stakes are high, and the economic impact of stolen trade secrets is a clarion call for stronger protections and proactive defence strategies.

Cybercrime

Cyberweapons used today

The dominant ‘ingredient’ present in a trade secret theft attack is data exfiltration. Unlike attacks such as ransomware, or Denial of Service, an attacker targeting a company’s trade secrets aims to be undetected throughout and after the attack. This profile of an attack is akin to the operations and behaviour exhibited by Advanced Persistent Threats (APTs). Another significant risk is from insider threats, namely employees, partners, and third parties in general who already have legitimate access to the organization’s systems.

How AI supercharged these cyberweapons

AI has significantly amplified the sophistication and effectiveness of trade secret theft attacks, particularly through enhanced spear phishing capabilities. AI-powered language models can now generate highly convincing, personalised phishing emails that mimic writing styles, reference specific industry terminology, and incorporate contextual details gathered from social media and public sources. Machine learning algorithms can analyse vast amounts of data to identify optimal targets, timing, and attack vectors, while automated systems can conduct reconnaissance at unprecedented scale and speed. AI also enables dynamic attack adaptation, where malicious systems can modify their behaviour in real-time based on

> **AI has significantly amplified the sophistication and effectiveness of trade secret theft attacks, particularly through enhanced spear phishing capabilities**

defensive responses, making detection more challenging. Furthermore, deepfake technology and voice synthesis can create convincing audio or video content for social engineering attacks, while AI-driven automation allows attackers to manage multiple simultaneous campaigns against different targets. Perhaps most concerning is AI's ability to help attackers blend malicious activities with normal network behaviour patterns, making the stealthy, long-term data exfiltration characteristic of APTs even more difficult to detect through traditional security monitoring systems.

How cyberweapons can be/have been used to steal trade secrets

Hacking a server to obtain a trade secret

Trade secrets in digital form, such as the formula for a breakthrough drug that has not yet been patented, are typically stored on a server that is armed with firewalls, encryption, and data logging. Trade secret owners use these tools to limit who has access, restrict the means of access, and to track who accessed the trade secrets and how much data was accessed at any given time.

A trade secret thief may use AI-enabled machine learning and adversarial neural networks to attempt to detect and decode the encryption used by the trade secret owner and circumvent the server's firewall. Once breached, the thief may then deploy AI-enabled APTs into the owner's network to wait until the data traffic on the server peaks so as to reduce the likelihood of detection during the exfiltration process of the trade secret. Using these cyberweapons, the thief could steal the aforementioned drug formula before its true owner had the opportunity to patent and market the drug.

AI-enabled phishing emails/communications

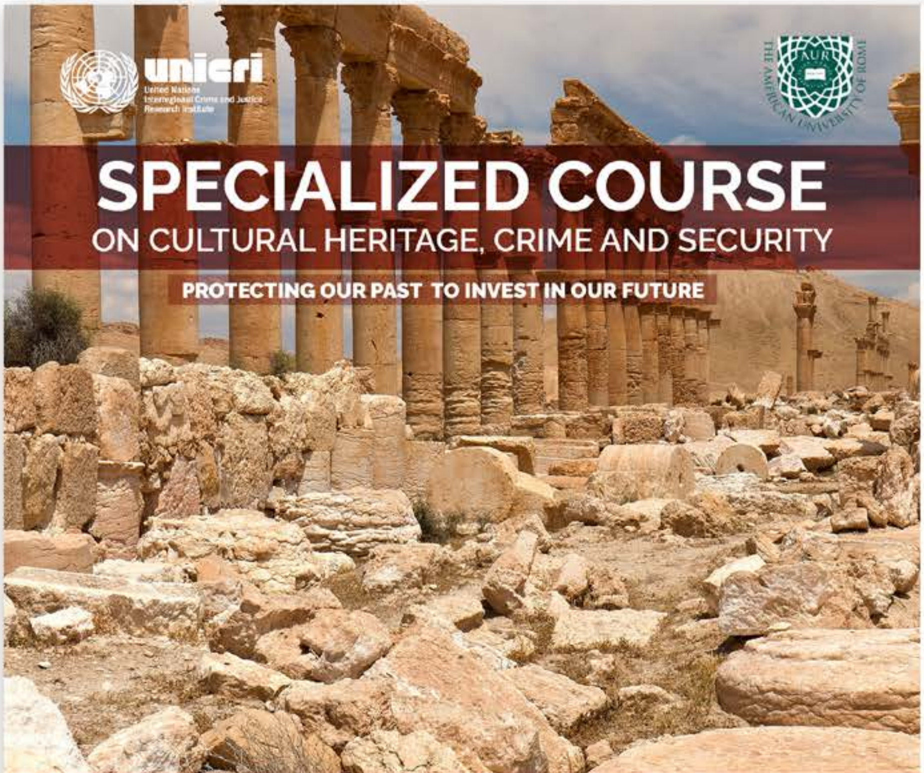
Some trade secrets, such as pre-release music albums or movies, are stored on servers with access limited to only a small team of employees. To identify the weakest employee with access to the trade secret, a trade secret thief may use AI-enabled automated systems to conduct rapid reconnaissance and determine to whom a phishing email should be directed. Once that employee is identified, the thief can implement AI-enabled deepfake technology to imitate the voice of the CEO of the company instructing the employee to disclose the trade secret via email. In this scenario, the thief could use the same AI-enabled cyberweapons referenced in the previous scenario to hack into the CEO's email account. Once the duped employee sends the email attaching the trade secret, the thief unlawfully accesses the CEO's email account (without authorisation) and downloads the trade secret. In this way, the thief

ABOUT THE AUTHORS

Kenneth Wright has a MSc in Information Security and previously served as a senior police officer but for the last 26 years has worked with governments, law enforcement and the private sector - in over 70 countries - to protect and enforce intellectual property (IP). During this period, he has prepared national IP strategies, drafted IP legislation, delivered IP capacity building and investigated IP crimes.

Vasilis Katos is Professor of Cyber Security and lead of Bournemouth University's Computer Security and Incident Response Team, BU-CERT. Prof. Katos specializes in digital forensics for intellectual property crime investigations. His work focuses on applying cybercrime and cybersecurity incident response practices to online investigations of IP crime.

John H. Zacharia is the Founder of Zacharia Law PLLC, a law firm dedicated to helping clients combat cyber theft and protect and enforce their intellectual property rights. Previously, as the Assistant Deputy Chief for Litigation of the Computer Crime and Intellectual Property Section (CCIPS) of the United States Department of Justice's Criminal Division, John was responsible for supervising all of the intellectual property and cybercrime prosecutions by the Section's 40 attorneys. While at CCIPS, John became one of the most experienced federal prosecutors of intellectual property crime in the country.



Join

the **United Nations Interregional Crime and Justice Research Institute** and **The American University of Rome (AUR)** for an in-depth program to safeguard cultural heritage in a time of crisis.

Explore the legal, political, and criminal challenges of protecting cultural property amidst conflict, looting and trafficking.

Info

- **Expert insights.**
- Practical **exercises** and **simulations.**
- Real-world **case studies.**
- Certificate of Participation issued by **UNICRI** and **AUR.**

The online format offers flexibility, bringing together participants from around the world for a truly global classroom experience.

English | Online | Students, Post-Graduates and Professionals

Be part of the global movement to safeguard cultural heritage!

Join

the **United Nations Interregional Crime and Justice Research Institute** and the **Italian Society for International Organization (SIOI)** for a dynamic hybrid program to safeguard truth in the digital age.

Address the legal, political, technological, and ethical challenges of misinformation, disinformation and hate speech.

Info

- **Expert insights.**
- Practical **exercises** and **simulations.**
- Real-world **case studies.**
- Certificate of Participation issued by **UNICRI** and **SIOI.**

This hybrid program allows for all students to have an immersive and adaptable experience, in a truly global classroom.

English | Hybrid (Rome or Online) | Students, Post-Graduates and Professionals

Take action to safeguard the digital information ecosystem. Be part of the solution!