# The Effects of Strain on Data Theft

legacv

December 1, 2024

**Abstract**

This paper explores Merton's 1938 Strain Theory (ST) and Agnew's 1992 General Strain Theory (GST) as functions that can be applied to cybercriminal actors that thieve and leak data; namely, the Shadow Brokers (TSB). The paper will first provide an overview of TSB's history and activity as a cybercriminal group and one of their famous cases of data theft from the National Security Agency (NSA), then explanations of Merton's and Agnew's theories. The paper will then seek to relate the two by examining the potential strains and stressors leading to the actions of the cybercriminal group with regards to the data leak and TSB's place in society with relation to Merton's postulations about success and cultural value. Finally, other works relating to cybercrime as a manifestation of Strain Theory will be explored, and their connections to this work and the future of the field will be elaborated upon.

## The Effects of Strain on Data Theft

*Data theft* is a cybercrime that is characterized by the unlawful obtainment of proprietary or sensitive data, and oftentimes the subsequent sharing of that data with a wider audience not originally privy to the data. *Data* can encompass many types of information; personally identifiable information (PII), credit card information (CCI), health information, usernames, passwords, trade secrets, and much more. Data can also include things like code or executables: items that an organization has developed and kept to themselves, which is common among technological or governmental organizations, as well as other institutions that perform research and development in the technological sphere.

Data theft can be committed by anybody, from an individual, disgruntled insider in an organization to hacktivists to organized nation-state movements. And, more importantly, data can be stolen from anyone. “An average of 25,575 records” (Alnuaimi & Alawida, 2023, p. 1160) are exfiltrated by cyberterrorists in every incident, where the end goals can be “extortion and espionage” (Alnuaimi & Alawida, 2023, p. 1160). The business of data theft can be lucrative, as well; individuals or organizations holding onto important or revered proprietary information can charge as much as a buyer is willing to pay for it or extort the victim organization for ludicrous amounts of money in exchange for a promise not to leak it (Alnuaimi & Alawida, 2023).

This is in part what makes data theft so compelling. It has its parallels to real-world theft; the criminal can either use what they bought to advance themselves and their situation, or they can resell it to someone who could get more use out of it, thereby making themselves money to fund their next heist. Cybercriminal organizations make livings off of posting breached data to forums, selling it to bidders, or using zero-days they found to exploit an exponentially higher number of companies for their money.

Another compelling piece of data theft is that it can be done en masse. With other high-return cybercrimes, such as fraud, it takes a significant amount of effort to collect a person's details, build a false identity, and perform transactions in their name. Data theft can potentially obtain millions of records in the same time that it takes to defraud a handful of individuals, making it much more effective in terms of the ratio of time spent to reward earned.

Strain Theory, proposed by Robert Merton in 1938, states that there are culturally valued objectives in an individual's life and socially accepted means of obtaining those objectives; in addition, when strains caused by society act upon individuals, they respond in one of five ways. Agnew's General Strain Theory, proposed in 1992, elaborates on this by providing types of strain, and again stresses that external pressures are great motivators for individuals to act in a delinquent manner. The delinquent manner at hand is, as discussed, the crime of data theft; following, the purpose of this paper is to explore whether Strain Theory and General Strain Theory as proposed by Merton and Agnew explain data theft by cybercriminal organizations.

**Case Study**

The Shadow Brokers (TSB) are a cybercriminal group made famous by their data theft and leakage from sensitive sources and flippant attitude about the aforementioned crimes when confronted. They appeared in the cybersecurity sphere in 2016, with their debut data being a "series of hacking tools and computer exploits […] from the NSA" (Schneier, 2017, para. 4) dating back to the fall of 2013.

In his 2017 essay *Who Are the Shadow Brokers?*, Bruce Schneier postulates that TSB are neither whistleblowers from within the NSA nor disorganized hackers who happened upon the information and shared it. The gap between the timestamp on the initial leaked data and the time of leakage would prove an ineffective schedule for whistleblowers, and a (smart) hacking group

would not have leaked the data at all; rather, they would have kept it for themselves as a form of "cyber-Kryptonite" (Schneier, 2017, para. 8). Therefore, he proposes that TSB is made up of nation-state actors who are both able to access the information due to resource availability (knowledge, money, time) and have the willingness to leak it—a group with the confidence that drawing ire from the United States' government would lead to no negative consequences. This implies a group so assured with their own tactics and secrecy that they have no issue bragging about their theft and selling their data very publicly.

One arm of their assurance is their payment method. Like many cybercriminal groups and individuals seeking to maximize anonymity with digital transactions, they use Bitcoin as their cryptocurrency of choice to receive, transfer, and use the money that they earn from selling their data leaks. They use disposable wallet addresses and mixing services as obfuscation techniques in order to minimize their chances of being traced through the blockchain, enabling members to live with their earnings in peace (Na, Kim, & Shin, 2018).

As previously mentioned, TSB became famous through their data theft—though one leak in particular delivered them their stardom. EternalBlue, a vulnerability in the Windows SMB protocol, was originally found and developed by a group known as the Equation Group—or, more accurately, members of the National Security Agency (Loleski, 2018). They privately informed Microsoft of this vulnerability in early 2017, leading Microsoft to publish bulletin MS17-010 to patch it before it was publicly discovered. However, in April of 2017, the Shadow Brokers made posts on multiple social media sites claiming that they had vulnerabilities found by the Equation Group (including EternalBlue) and that they would leak them to buyers. In particular, the "OH LORDY! Comey Wanna Cry Edition" post on Steemit insulted the Equation

Group and those who didn't believe in the Brokers' power (Shadow Brokers, 2017) as well as advertised the sale of the stolen data.

TSB did end up leaking EternalBlue, though the package contained much more; TSB also released EternalChampion, EternalRomance, and EternalSynergy, among others (Goodin, 2017). The leaked EternalBlue exploit was used to carry out the NotPetya attacks and WannaCry ransomware attacks later that year. NotPetya affected "as many as 60 percent" (Stoddart, 2022, p. 377) of the systems in Ukraine, and WannaCry affected "around 200,000" (Stoddart, 2022, p. 376) machines globally. Though these attacks didn't come from the Shadow Brokers themselves, they were carried out with the information that the Brokers leaked, which in turn means that the footprint of their impact grows wider and wider.

The most recent TSB activity on Steemit was in 2017, and since then, no major data theft or leakage has been attributed to them. The assessment to be made is that TSB was a brief coalescence of high-motivation, high-ability hackers who may or may not have been backed by a nation state. It is most likely that the members of TSB have scattered themselves across other cybercrime groups, renamed themselves, and cast off their old identities, further ensuring their secrecy while maintaining their relevancy in cybercrime circles.

**Theory**

Strain theory was originally articulated by American sociologist Robert K. Merton in his 1938 work *Social Structure and Anomie*. He first asserted two things: that society cultivates cultural values in the form of goals or ideals that members of that society should strive to achieve; and that society defines acceptable means of achieving those goals: hard work, education, moving through the correct legal channels, abiding by social norms, and so forth. However, due to unequal power structures that exist in society, not every member is able to

achieve these goals. Rather than simply drop the goal, individuals are culturally pressured to obtain it at any cost, which then produces deviance—rejection of the typical means (or, in some cases, rejection of the typical ends). It can be said, then, that deviance is not always caused by personal dispositions, but by external strain (Merton, 1938).

Merton went on to argue that there are five ways that individuals adapt to strain. *Conformity*, generally seen as the non-deviant approach, seeks to achieve culturally valued goals through socially acceptable means. *Innovation* seeks to achieve culturally valued goals through socially unacceptable means, for example achieving wealth through extortion. *Ritualism* and *retreatism* both forgo culturally valued goals; a ritualist does not necessarily seek to achieve them but steadfastly sticks to socially approved channels anyways, perhaps due to fear of nonconformity. A retreatist shuns both ends and means and seeks a way to break free of societal expectations, which can manifest in disengagement and does not necessitate violence or active struggle. Finally, *rebellion*, somewhat like retreatism, shuns both ends and means and seeks to replace them with alternative goals and channels (Merton, 1938).

Merton's theories were refined by American criminologist Robert Agnew in 1992 with *Foundation for a General Strain Theory of Crime and Delinquency*. According to Agnew, strain, or stress, increases the likelihood of individuals of a society adapting with crime and delinquency, especially when other channels of properly confronting and treating strain are unavailable. The two types of strain Agnew proposes are objective strain that is widely disliked among a group (for example poverty) and subjective strain that is disliked by the individual that is currently experiencing it. He went on to expand two more types of strain, vicarious and anticipated. Vicarious strain occurs when one individual's strain indirectly causes stress in another, for example a child and their parent; anticipated strains occur when a strain has not

occurred and is not currently occurring but is expected or predicted to occur, for example fear of job loss (Agnew, 1992).

In addition, there are three types of deviance-producing strain (separate from objective and subjective) that Agnew proposes: failure to achieve goals, the loss of positive stimuli, and the addition of negative stimuli. When an individual experiences one or more of these, it leads to negative emotion, which can drive deviant behavior.

There is a caveat where two individuals can respond differently to the same strain depending on their personal dispositions, access to resources, and support. For example, if two individuals recently lost their primary income sources, one with a system of social or monetary support could adapt via finding a new job, while the other who lacks it might feel pressured to turn to crime or theft. These variations emphasize that strain is not the sole predictor of deviance, and that the importance of personal and contextual factors cannot be understated.

## Discussion

The theories proposed by Merton and Agnew, though developed without relation to technology, can be applied to current forms of cybercrime and cybercriminals to attempt to understand their behavior; namely, the Shadow Brokers in their 2017 National Security Agency data leak.

In order to analyze TSB's behavior using that framework, it is necessary to deconstruct the most important elements of both theories and classify the Shadow Brokers' actions as manifestations of those theories. This includes a discussion of individual vs. group action; TSB's place in society and cyber-society; their goals, strains and types of strains under the two frameworks; and a comparison of their actions with similar physical/non-cyber actions that have been analyzed under ST and GST.

For the purposes of this paper, is easiest to classify TSB as an "individual" rather than a collection of individuals. The individuals that make up TSB are presumed to have the same or similar motives to each other (at least, similar enough to work towards the same goal); they perform actions as a collective; and their public appearance is one unified front with a designated speaker rather than a posted collection of thoughts from each of their members.

TSB is in a unique position in cyber-society in the present day. Despite being inactive for several years, their notoriety persists due to the magnitude of their impact on cybercrime and data theft. Maybe, then, the definition of TSB can shift further—maybe they can be classified as an era, or a movement, rather than an actor; the longer TSB doesn't resurface, the more that argument could be made. Other cybercriminal groups, regardless of whether or not they are nation-state actors, could hold TSB's actions in high regard; they steal quite flippantly from one of the most powerful organizations in the world, and trade that data for money. That cements TSB's reputation as a skilled actor which other groups could want to emulate.

Moving past the examination of the effects of TSB's data theft, it becomes necessary to ascertain the goals of TSB—even if the group itself is no longer active, mimics continue down the same path, and knowing their motivations becomes key to minimizing their destruction. TSB's actions' intersection with ST and GST are of particular interest, so it is worthwhile to examine the potential strains that acted on TSB.

It can be somewhat difficult to pinpoint specific strains affecting such a secretive group without any sort of direct contact; however, they can be estimated from publicly available information and statements given by the group. For example, the Steemit post from the EternalBlue leak—"OH LORDY! Comey Wanna Cry Edition"—provides much-needed context as to the feelings of TSB at that point in time. Since TSB was originally trying to sell their

information to the highest bidder, as they had in the past, it's safe to conclude that they are suffering from the strain of the lack of money, which under Agnew would be both objective and a failure to achieve goals. TSB likes to question why they are facing this strain, saying, "TheShadowBrokers is asking selves, selves why is no peoples making offer on theshadowbrokers equation group warez?" (Shadow Brokers, 2017), indicating that TSB may be frustrated with their fruitless attempts to sell their wares especially since there is "much great interest in free warez" (Shadow Brokers, 2017). This frustration points to there being a valid strain on the group that is pushing them to commit data theft to resolve.

With the information presented, under Mertonian strain theory, TSB would be classified as an innovator. They reach for culturally valued goals—money, notoriety—through criminal, and therefore socially unacceptable, means, which falls very neatly in line with Merton's definition of innovation as a strain response. That's not all they do, however. The undercurrent of the hacking community, from its inception, has included the reshaping of social norms and the desire to implement new practices in place of old, outdated hierarchies (Thacker, 2004). As members of and contributors to hacking culture, it would be remiss of TSB to not hold this mindset throughout their activity—the mindset, of course, being reminiscent of Mertonian rebellion. Though it was established that TSB does strive for culturally valued economic status, the fact that they publish any of their wares for free points to their distaste for the 'system' as it stands. This is once again evidenced through the Steemit post, where they say, "This is theshadowbrokers way of telling theequationgroup 'all your bases are belong [*sic*] to us'. TheShadowBrokers is not being [*sic*] interested in stealing grandmothers' retirement money. This is always being [*sic*] about theshadowbrokers vs theequationgroup" (Shadow Brokers, 2017,

para. 13). This becomes contextualized once it is made clear that the Equation Group is, as Loleski (2018) posited, an extension of the NSA.

Had the NSA not been attached to the U.S. government—say, if TSB had stolen data from another cybercriminal organization—it might have boiled down to petty theft, a longstanding rivalry for notoriety, or 'turf wars.' However, looking at the feud from another lens, it could be said that TSB is trying to undermine the power of the U.S. government. TSB, as they claim, is not interested in the theft of personal funds or data as a means of making money. It is important to them that the data specifically came from the Equation Group, and it is important that the world knows that the Equation Group—the U.S. government—is not invulnerable to hacks (Shadow Brokers, 2017). This rejection and reclamation of power points to TSB not only being innovators under Merton, but also rebels seeking to tear down existing structures and thereby exhibit deviancy by rejecting the ends.

Previous work on this topic does not specifically delve into data theft, but rather a broader collection of potential cybercrimes that could be committed by strained individuals. Mohamad, Hamin, Nor, & Aziz, in their 2024 work *Selected Theories on Criminalisation of Hacking*, explore GST as one of the many potential explanations for deviant behavior with respect to hacking. They posit that all three types of strain discussed by Agnew could apply to hacking: the inability to obtain desires such as money; the loss of positive stimuli such as relationships or social standing; and the addition of negative stimuli such as toxic workplace or social environments. These, combined with personal disposition and access to information, could lead an individual to begin hacking to find a sense of empowerment or retaliate against power structures (Mohamad, Hamin, Nor, & Aziz, 2024). Such concepts are easily applied to the TSB

case study: TSB had an inability to obtain money or notoriety and/or were feeling pressured by the NSA's power, so they retaliated.

Due to the clear connections that can be made between the defined strains and TSB's actions, it can be concluded that Merton's Strain Theory and Agnew's General Strain Theory can adequately explain the actions of the Shadow Brokers with regards to this case study. It should be noted that the study is not the only example of the Shadow Brokers stealing data from the NSA, and in some cases, TSB didn't even make an effort to sell the data (Schneier, 2017). This could point either to a stronger application of Merton's *rebellion* classification of TSB, or to external driving forces that motivate TSB and have nothing to do with strain. Certainly it is possible that individuals not experiencing monetary or social strain hack and leak data, and without knowing the exact composition of TSB, it is impossible to say for certain that every member was acting due to the effects of strain throughout the entirety of TSB's career. However, based off the evidence given by TSB's Steemit post, it is clear that monetary strain was a driving force behind the EternalBlue leak and that TSB has a disposition towards rebellion. Those two facts allow an adequate characterization of the EternalBlue leak being a manifestation of the strain placed upon the Shadow Brokers.

As mentioned, the EternalBlue leak was not the only leak made by TSB, and it certainly was not the only time that sensitive data was leaked from a government entity. Many more groups, including hacktivist groups, have stolen and published data from the U.S. government and other national entities; whether Strain Theory and General Strain Theory apply in those cases could be prudent to study, especially considering the political angle briefly touched on in this paper. Other types of cyber and technological crime might match up far more neatly with ST and GST; for example, Chism & Steinmetz (2018) points to crimes like piracy, fraud, and even

cyberstalking as viable manifestations of the theories. Furthermore, Merton and Agnew were not the only ones to describe Strain Theory and General Strain Theory. The theories have been advanced most recently by Jie Zhang in his 2019 text *The Strain Theory of Suicide*, which at its face may not have a connection with cybercrime but could be explored through its ties with cyberharassment and cyberstalking.

## Conclusion

The theories of Merton and Agnew, though not created with the advent of technology, are universally applicable to the human condition. It can be said that cybercrime is a rehash of traditional criminal practices with new technologies and methods behind it; ransomware still demands a ransom, website defacement is vandalism, and data theft is still theft. Therefore, the theories discussed can be quite cleanly applied to new technical actors and scenarios, such as the TSB case study here. The Shadow Brokers are, in many ways, subject to the same strains and culture as non-technical people: lack of and desire for money, desire for fame, fear of obscurity and irrelevancy. For these reasons, they and their actions can be analyzed under the ST and GST frameworks. There are more nuanced discussions to be had, both with regards to related cybercrime and cybercriminal organizations and expanded versions of the two theories; hacking as a field of study is still relatively new, and therefore many connections between old theories of individual behavior and new techniques of cybercrime still have yet to be drawn.

**References**

Agnew, R. (1992). Foundation for a General Strain Theory of Crime and Delinquency. *Criminology, 30,* 47–88. https://doi.org/10.1111/j.1745-9125.1992.tb01093.x

Alnuaimi, R. A., & Alawida, M. (2023). Understanding Cyberterrorism: Exploring Threats, Tools, and Statistical Trends. *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 1155–1162. doi:10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361351

American Psychological Association, issuing body, & American Psychological Association, issuing body. (2020). *Publication manual of the American Psychological Association : the official guide to APA style.* (Seventh edition.). American Psychological Association.

Aïmeur, E., Brassard, G., & Guo, M. (2022). How data brokers endanger privacy. *Trans. Data Priv.*, 15, 41-85.

Chism, K. A., & Steinmetz, K. F. (2017). Technocrime and strain theory. In *Technocrime and criminological theory* (pp. 66-84). Routledge.

DiPersio, D. (2024, May). Selling Personal Information: Data Brokers and the Limits of US Regulation. In I. Siegert & K. Choukri (Eds.), *Proceedings of the Workshop on Legal and Ethical Issues in Human Language Technologies @ LREC-COLING 2024* (pp. 39–46). Retrieved from https://aclanthology.org/2024.legal-1.7

Goodin, D. (2017, April 14). *NSA-leaking Shadow Brokers just dumped its most damaging release yet*. Ars Technica; Ars Technica. https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-

release-yet/

Loleski, S. (2018). From cold to cyber warriors: the origins and expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers. *Intelligence and National Security, 34(1),* 112–128. https://doi.org/10.1080/02684527.2018.1532627

Merton, R. K. (1938). Social structure and Anomie. *American Sociological Review, 3,* 672–682. https://doi.org/10.2307/2084686

Mohamad, A. M., Hamin, Z., Nor, M. Z. M., & Aziz, N. A. (2024). SELECTED THEORIES ON CRIMINALISATION OF HACKING. *INTERNATIONAL JOURNAL OF LAW, GOVERNMENT AND COMMUNICATION (IJLGC)*, *6*(22). Retrieved from https://gaexcellence.com/ijlgc/article/view/2119

Na, S. H., Kim, K., & Shin, S. (2018). Knowledge Seeking on The Shadow Brokers. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3243734.3278512

Schneier, B. (2017, May 23). *Who Are the Shadow Brokers?* The Atlantic; The Atlantic. https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In: *Cyberwarfare*. Palgrave Studies in Cybercrime and Cybersecurity. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-97299-8_6

Thacker, E. (2004). Hacker Culture. *Leonardo*, *37*(4), 345-346.

Zhang, J. (2019). The strain theory of suicide. *Journal of Pacific Rim Psychology*, *13*. https://doi.org/10.1017/prp.2019.19.