Deep Science Publishing
https://doi.org/10.70593/978-81-988918-0-8_9

DeepScience
Open Access Books

Chapter 9: Identity theft protection in a hyperconnected world: How insurance can safeguard your digital identity

9.1. Introduction

One of the key features of the modern world is that it is hyperconnected. Everyone, including young children, owns a personal digital assistant, a smartphone, that is always on and connected with the Internet and with the people they are in contact with most frequently. We do everything online, from banking to shopping and travel reservations. Recent events have accelerated the move towards doing even more on connected devices, including telemedicine consultations, online therapy, and schooling. This has caused a dramatic increase in the amount of time we spend in digital environments, with an exponential rise in the amount of data companies can collect about us. In this highly-connected, highly-tracked world, a multitude of inherent risks to our digital identities have emerged. Anonymity is no longer an option, nor would we want it to be. We cannot opt out of the records we leave behind every time we go online, records that can be freely traded across the Internet marketing landscape, records that are equally available to criminals, marketing companies, and those who wish to do us no good (Englezos, 2022; Ghadge, 2024; George, 2025).

While there is a certain appeal to this hyperconnected world, the new vulnerabilities we expose ourselves to are troubling. What happens when, for whatever reason, that connectivity is interrupted? What happens to the records created and maintained by companies during that time of disassociation? Companies thrive on that data, and, if something impedes the algorithm from collecting those data, what does a company do? Steps must be taken to protect the rights of the individual user, steps that are not available today. And while companies rush to get their share of the profits from hyper conduit activity, they never pause to consider what havoc a temporary interruption in service could cause.

Consumer reports of fraud and identity theft skyrocketed in 2020. Identity theft soared for reports, while reports of fraud increased. While IRS tax fraud, credit card fraud, and other familiar types of identity fraud still account for the vast majority of fraud cases, a new hybrid approach has sprung to want and more clandestine identity theft. Credential stuffing is the practice of using a set of stolen credentials, such as username and password, to attempt to take over accounts. Credential stuffing only works when people use the same credential sets across multiple services (Sule et al., 2021; Shah, 2022; Weippl & Schrittwieser, 2024).

Fig 9.1: Insurance Can Safeguard Your Digital Identity

9.2. Understanding Identity Theft

Digital identity theft is primarily about the unlawful use or appropriation of someone's personally identifiable information (PII), such as their full name, social security number, bank account information, address, or driver's license number, among a slew of others. But the digital aspect of identity theft stems from the fact that so much PII is now stored online in such a variety of ways: on social media sites, with cloud and data storage facilities, at online retailers, with financial institutions and payment processing services, and at any business which customers give their personally identifiable information to. Each of these centers, however secure their data protection protocols are, is a potential target for would-be identity thieves.

For example, in 2020, it was indicated that of the nearly 77 million Americans who reported having been victims of identity theft, around 27 million – or roughly 35 percent – were victims of identity theft relating to online filing of unemployment benefits, or of thieves requesting pandemic-related economic impact payments that were misrouted because of stolen identities. Another 15 million indicated that someone had either hacked or impersonated them, and attempted to gain illicit access to their employer's tax records or payroll accounts. But despite the prevalence of digital identity theft, it is generally not the most common form of identity theft Americans encounter in the pandemic era; more Americans still apparently fall victim to the more traditional form of physical identity theft, with credit card fraud being the single most commonly encountered variant of that type of in-person identity theft.

9.2.1. Definition and Types of Identity Theft

Identity theft occurs when an individual's personal identifiable information or PII is recorded by another individual without permission for the purpose of committing fraud or related crime. The victim, also termed the identity theft target, suffers financial harm, emotional distress, and repercussions when the criminal conducts fraudulent transactions in the victim's name. Digital data is especially vulnerable to theft. Theft methods include data breaches, skimming or phishing to capture online passwords or PII, malware, sim swaps, or simply collecting stolen physical credit cards or passports. Threat actors can use this data to make fake identification, passports, or social security cards; make fake credit cards bearing the victim's name; drain or hijack bank accounts or credit card accounts tied to the victim; open new accounts in the victim's name; or acquire loans or lines of credit through impersonation. Cybercriminals are increasingly using the dark web to love PII for sale. These fraudulent acts can occur in the victim's name across geographic borders. Victims can take years to untangle the fraudulent transactions conducted in their names.

Many studies have sought to understand the different facets of identity theft, offering definitions. For forensic understanding, one helpful typology looks at how identity production and identity fraud differ at different levels. Identity theft occurs in three different forms: 1) social identity theft; 2) personal identity theft; and 3) digital identity theft. Social identity theft borrows or steals information from social accounts, so one actor can attract followers and post messages to impersonate that awakened person or organization, driving followers to become co-conspirators or enabling social hacking. Dramatic examples are the use of social media to impersonate news outlets or celebrities to spread fake news, scams to obtain followers, then to impersonate people's accounts, or recruiting co-conspirators. As well, more serious criminal activity might involve identity signatures of public leaders that are stolen and published.

9.2.2. Statistics and Trends in Identity Theft

The reported data breaches in the US in 2020 leaked nearly 300 million records. Phishing is the leading cause of identity theft. These breaches exposed the personal information of more than 5.2 million people. Because of COVID-19, online services experienced a surge in usage. This expansion, coupled with remote work at companies, which increased connectivity and remote collaboration, created larger surfaces for attackers to exploit. Web application attacks accounted for 40 percent of all breaches. The pandemic and the economic fallout also created situations ripe for exploitation by scam artists. More people experienced financial hardship or exposure to the virus. Targeting the disinformation-shocked public with fears of infection or economic hardship created especially bad conditions. Businesses and banks also spent a significant amount over the losses.

9.3. The Role of Technology in Identity Theft

With the continuous advancement of technology, digital identity has become one of the main frontiers in the growing battle between fraudsters, hackers, cybercriminals and the police. Identity theft has existed throughout history, but the way it is taken today is unique and completely different from previous cases of fraud against individuals. Today, with the capillary penetration of the Internet, identity theft has been sadly democratized. Huge rows of people all around the world are victims of identity theft. Following a well-defined process, crooks can gather all the data, documents and information they need to impersonate the victim and make use of their stolen identity for fraudulent purposes. For this very reason, identity theft has become one of the most criticized and combat issues, also because the consequences of being a victim of this kind of fraud are very serious. By taking advantage of the technological instruments at the forefront of Machine Learning, Data Science and Artificial Intelligence, banks and financial institutions are developing increasingly effective detection systems. Also, in order to avoid being a victim, it is recommended to have physical protection of the data stored in the computer.

Cybersecurity Vulnerabilities. Research has shown that one significant barrier for many victims, especially seniors, is the notion that they are not ‘tech-savvy’ enough to protect themselves from frauds seeking to exploit technology to commit acts of fraud. For those who are ‘tech-savvy,’ they may not be aware of the different technologies criminals are utilizing to defraud individuals. With studies showing that attacks on users’ digital security are rising with increased prevalence and intensity, e.g., phishing and email compromise. While tech companies are making strides in securing their platforms, it is inevitable that they may also struggle to keep pace with emerging threats. Indeed, with recent high-profile breaches making headlines, it is no longer enough to say ‘phish with

caution'. Users must also remain vigilant about what they see as trustworthy services, including both traditional banks and crypto financial platforms.

Fig 9.2: Role of Technology in Identity Theft

Social Engineering Tactics. Cybersecurity cannot solely be the responsibility of tech companies. Users also play a key role in maintaining the safety and security of their digital identities. Criminals employ social engineering tactics to make their actions appear as legitimate communication, often mimicking trusted contact from the victim's life.

Private citizens must enlist the participation and cooperation of corporations and businesses, and vice versa. Furthermore, in most cases of information and identity insecurity, the perpetrators involved are hackers with expert knowledge of computer systems, facilities, and networks. The hacker community is thriving, and is so large, self-contained, and adept that employing law enforcement to combat computer crimes is problematic. Cybercriminals are known to penetrate the networks of businesses and bank accounts of governments, companies, and private individuals for monetary gain. Attempts at enforcing laws against digital theft are occasionally also met with criticism for not being necessarily in the best interest of society.

9.3.1. Cybersecurity Vulnerabilities

The increased use of the Internet, smartphones, and the proliferation of cloud computing have created vast opportunities for identity thieves. With the help of technology and specialized criminal communities, unauthorized individuals can instantly acquire, sell, and profit from stolen identities. These and other cybercriminal activities are undermining personal relationships and interactions and criminalizing the online experience. Billions of records containing personal and financial details such as birth dates, social security numbers, bank account numbers, passwords, credit card data, and mortgage information are readily accessible, awaiting illicit purchase. Cybercrimes are also becoming increasingly structured and organized, several warranting classification as cyberwar. Hackers are amassing sensitive ID information and damaging the cyber operations of banks, businesses, and governments, and openly stealing large sums of money.

Certain information security weaknesses favor the criminal usurpation of identities. Cybercriminals are finding new ways to avoid detection and capitalize on the laxity of information guardianship by businesses and families. Not one method of identity theft protection by itself is sufficient to guarantee safety from falling prey to such crime.

9.3.2. Social Engineering Tactics

Cybercriminals regard social engineering as a privileged path for achieving their objective due to the reduced level of cybersecurity effort required in its execution. Classic examples such as phishing, vishing, or pretexting still dominate this domain, generally due to the easy availability of tools and resources in underground communities to automate and massively deploy these attacks. While giving the impression of a simple process, the art of social engineering is a complex task that implies a series of steps to be executed for an attack to be successful. It is not enough to possess the availability of tools; attackers need to have the knowledge and experience to maximize the probability of success. Social engineering aims to gain the victim's confidence in order to obtain sensitive information regarding their identity, whether by assimilating the trait of the interlocutor or using the prestige of a reputed and trustworthy identity.

Taking this further, the attacker should personalize the information to be sent to increase the chances of success. Hence, this stage requires a prior reconnaissance and profiling research process to collect the information they will use against the victim. Numerous social engineering attacks have been very successful among employees of large corporations and banks, culminating in the theft of millions. It is also very common for attackers to use social engineering on friends or family of the victim in order to establish

the appropriate level of trust with identityuser to whom they have revealed personal data and use these same people to impersonate them, reducing attack success probability.

9.4. The Impact of Identity Theft

Although the increase in identity theft reports may be interpreted as a reflection of growing public awareness of such crimes, it is much more convincing to be understood in terms of the rapid growth of the crime with deplorable consequences for affected individuals. Estimates suggest over 33 million identity theft victims in the United States since 2016. Importantly, this great number is expected to have been boosted by the COVID-19 pandemic. Using online criminal activities to put together the pieces of victims' lives has become the easiest way for hackers and cybercriminals to steal identities without having to leave their homes. The emotional, psychological, and financial consequences for victims of identity theft can differ widely depending on the form the theft takes.

Victims often exhibit fearfulness, disappointment, disturbed authority, loss of control, increasing social withdrawal, depression, and many more feelings and emotions. Most violations within the social relational system caused by identity theft, such as loss of social prestige and damaged credibility, cannot be replaced easily or at all. Associating with relatives and friends can become aggravating. Besides, the emotional and psychological considerations associated with refuting identity theft differ from person to person and create extreme levels of stress. Various surveys confirm identity theft victims experience symptoms comparable to those seen in individuals suffering from post-traumatic stress disorder. Reports examining the general effects of the crime indicate that victims experience high levels of mental and emotional distress, as well as a deterioration in physical health.

The financial effects of identity theft can also last for years and incur great costs for their victims. Obtaining new documentation and mending damaged credit history can incur costs of several hundred dollars. Affected people may further incur different damages dependent on how their identities were exploited and the duration of the impersonation. More than 18 million identity theft victims incurred over USD 17 billion in out-of-pocket costs in 2018. Other research has shown the average cost for victimized persons to remediate and recover from identity theft to be over USD 6,000. Likewise, based on a survey applied to a national representative sample in Sweden, victims encountered out-of-pocket costs of more than EUR 1,000 on average.

9.4.1. Emotional and Psychological Effects

Experiencing identity theft not only incurs economic losses and long-term financial difficulties but may also provoke severe emotional responses and psychiatric disorders. Victims report feelings of violation, defilement, embarrassment, stress, anxiety, and insecurity; emotional distress lasting for months or years after victimization; and lower levels of subjective well-being. A host of post victimization consequences are also common: anger directed at the perpetrator; loss of time and trust, especially in strangers; social withdrawal; and consideration of relocation.

Victims report suffering from most of the typical symptoms of posttraumatic stress disorder, including depression, increased anxiety, sleep disturbances, and social withdrawal. Insecurity, trust issues, and anger may also stem from posttraumatic stress disorder. Some victims report suicide attempts and thoughts of physical revenge, and some become physically aggressive. However, heightened aggression or other types of risky behavior toward others may also be due to a third factor. Lack of trust in the authorities and symptoms of clinical depression may require the victim to undergo expensive psychiatric and psychological treatment.

Research shows that social interaction deficits are prevalent among identity theft victims. Communication with friends and relatives may ease the pain of victimization. Unfortunately, however, victims may not feel comfortable seeking help from relatives and friends or blame them for having "complicated" their lives. Having their problems validated and helped sufficiently might help them recover. Deprivation of social relationships might additionally escalate and lead to self-destructive behavior, culminating in serious psychological issues, including suicide and homicide. Academic research shows that social knowledge plays a prominent role in the post victimization phase; it is essential for the victims' ability to resolve and learn from their victimization.

9.4.2. Financial Consequences for Victims

The number of days is a well-known and broadly publicized statistic devised for use in reports. It indicates the number of days a victim needs to spend to restore a stolen identity to the level it was at before the incident. The estimate of $6,000 in lost victim wages is three times the average wage lost by any of the victims. It is burdensome to demonstrate that presenting such disparity may be misleading with respect to the real loss a victim endures. Recent survey analyses seem to indicate that the average cost incurred by the victims is more in the range of $2,500. However, the estimates are still more than three times lower than the indirect loss estimate reported. Victim wage losses and other estimated losses do not include the costs incurred by employers for displaced workers but only reflect the wages paid to victims by their employers. Either way, identity theft

can carry devastating effects on an individual's credit records, job prospects, and overall financial well-being.

Comparisons of the financial consequences of four types of scams on victims to non-victims using statistical tests revealed that the average financial loss suffered by identity theft victims was significantly higher than the average loss sustained by victims of shipping fraud. Specifically, identity theft victims lost roughly two-and-a-half times as much as shipping victims. The choice of scams was detrimental to the amount of loss incurred. More importantly, the financial consequences of identity theft were not only aggravated by the long recovery process but were also largely asymmetric. Identity and payment victims, for example, experienced longer recovery times, incurred higher recovery and out-of-pocket costs, and were more likely to have future money loss and other related issues compared to shipping and other transaction victims. All four groups, however, reported significant time loss and suffered anxiety effects.

9.5. Preventative Measures Against Identity Theft

Preventive measures in dealing with identity theft can be categorized into personal security practices and protective technology. The cost and effectiveness of mental security measures can vary significantly. Obviously adopting a minimalist approach to sharing personal data greatly reduces the opportunity for loss. For example, simply telling merchants and others that you do not want their information shared with any third parties is an important first step.

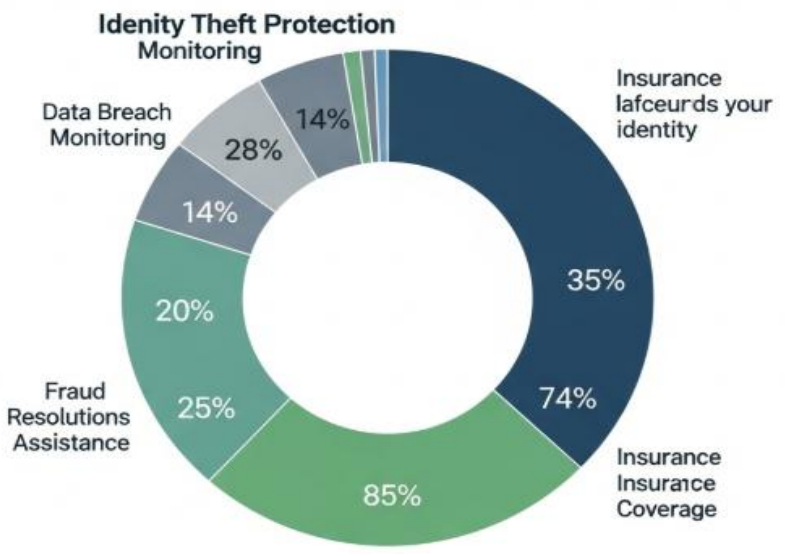

Fig : Theft Protection in a Hyper connected World

The same goes with on-line purchases. Before purchasing, check and ensure that the merchant has your expressed approval to store your personal data—the default is often to turn on that feature which is to the benefit of the merchant but contrary to your interests. Plus, carefully review any customer privacy and data storage policy from a merchant before deciding to purchase from them. Also, do not have the last four digits of your social security number show up on your bank debit card or the customer service number on the back of the card, and never let your debit card used as credit be processed without having to enter your secure code. Interestingly, research suggests that technology gives consumers a false sense of security. But technology used in a proactive manner can, in fact, provide a much greater measure of security. Strong passwords with sifting effects authorized access to some accounts and data are essential. Moreover, opting for a biometric login is highly advisable. If necessary, consider restricting access to your second-factor accounts to your first-factor accounts to create an additional security barrier to your access to your two-factor accounts and, if feasible, never access your two-factor accounts via Wi-Fi.

9.5.1. Personal Security Practices

The Garner group found that organizations in 2007 were forced to spend 611 billion USD due to security breaches that were mainly caused by identity theft. The number of cases is said to have increased in the past seven years or so. Improving your personal security practices can reduce your risks and may increase your chances of quickly discovering any problems. Here are some security practices that may help you.

Secure your personal information. Be careful with your Social Security number, and keep your driver's license number and credit account numbers private. Only give out these numbers when you are absolutely sure that the organization is legitimate and that the number is necessary. Even then you may want to check out how the organization will use the number. Many organizations can use other identifiers, such as a customer number, instead. Shred receipts and financial statements before you dispose of them. If you close an account, request that the organization send you written confirmation that the account has been closed and balance zeroed.

Never use your phone number as a password or personal identification number. Password protection is a good idea for access to electronic accounts, but all too often this action is neglected. Identity thieves can use your password to gain access to your e-mail, credit accounts, insurance, bank and retirement accounts. Using a weak password is the first step to exposing your personal information to potential abusers of identity. Passwords should be at least eight characters long, and the longer the better. A strong password will contain upper and lower case letters, a number, and a special character. Avoid using your name, birth date or other words or numbers that could be easily

guessed. Change your passwords frequently. Avoid using the same password for multiple accounts.

9.5.2. Utilizing Technology for Protection

While technology does play a primary role in advancing identity theft, it can also be utilized as preventative measures. Some effective use of technology includes: Safety Software – Utilizing safety software on your electronic devices allows you to create multiple levels of security against unauthorized users. Programs such as firewalls and directional services will prevent outside access to your computer network and track individuals accessing information from within your network. This provides effective defense against hackers. Anti-Virus/Anti-Malware Applications – Utilizing anti-virus and anti-malware applications as preventative measures allows you to utilize technology to stop attacks and risks that otherwise could result in identity theft. These software applications help filter out and protect you against phony email solicitors, prevent those viruses that capture your keystrokes from gaining access to your account passwords, and initiate alerts to notify you of unauthorized attempts to access your accounts. Additionally, these programs run background checks to identify fraudulent behavior on your computer or mobile device. Encryption Software – Many financial and identity management companies offer software programs to consumers for the express purpose of safeguarding sensitive consumer information. Utilizing software that encrypts sensitive files allows the consumer extra peace of mind in knowing that their personal and financial information is at lesser risk of being accessed through unauthorized means. Utilizing encryption software is particularly important for those who conduct transactions and send other public information through electronic means. Identity Theft Safeguards – There are several consumer-based safeguards that companies and organizations offer in an attempt to prevent electronic and financial fraud. Utilizing services that track and warn about potential unauthorized entrance into consumer accounts as well as those that perform background assessments and investigations of the public database related to credit and identity issues are two of the most important concepts in dedicating firm prevention tactics against the risk of current or future identity theft.

9.6. Insurance as a Safeguard

Although identity theft can involve harrowing experiences, the good news is that most people who are victims of identity fraud are protected by law. Such people generally pay little or nothing in the way of liability for the financial, tax, or medical accounts that

someone else opened or used. Unfortunately, although the laws exist to protect people, the rescue and remediation process can be tedious and lengthy.

This is where identity theft insurance can offer a solution and alleviate some of the anxiety and burden. Identity theft insurance is typically a product offered through an insurance company or a membership through a specialized account service provider to cover losses or expenses associated with restoring an identity that has been compromised. Such policies or memberships can assist with expenses related to identity restoration, including:

• legal fees for advice about or assistance with restoring a person's good name and credit record;

• notary and mailing costs to remit fraud affidavits to affected companies;

• long-distance telephone calls to dispute fraudulent charges or ongoing criminal activity;

• interpretations of accrued documents; and

• parental leave for any time spent resolving identity fraud issues.

Since identity theft insurance is typically associated with restoring, recovering, and remediating identity fraud damage rather than preventing identity fraud in the first place, people should also seek preventative solutions to identity theft.

9.6.1. Types of Identity Theft Insurance

Colloquially referred to as identity theft insurance, identity restoration services can help you get your original identity back in the event that your identity is stolen and cannot be restored on your own. However, the services are not actually considered to be insurance coverage, as they do not guarantee you any compensation if identity restoration takes a long time or even if it is not completely successful. Many major companies offer some form of this identity restoration service, but the coverage comes with lots of exclusions. Before purchasing a plan, be sure to examine all of the exclusions carefully. Be aware that most identity theft services will not reimburse you for any lost wages that may occur during the identity restoration process. Services that offer more comprehensive coverage may also come with hefty premiums that could be better spent on your own ID protection measures.

Even though these policies often lack coverage for the effects of identity theft, they remain popular among consumers. Insurers believe consumers would rather pay for a service to help restore their identity than do it on their own. And these restoration

processes can be long and complicated. State regulators continue to hear complaints about problematic identity theft policies that consumers purchase under the impression that they are buying insurance. However, the companies are filling these policies with exclusions, limits, and restrictions so that they are of little use in the event of an actual identity theft.

9.6.2. How Insurance Works in Identity Theft Cases

There are two types of identity theft insurance: first-party insurance and third-party insurance. Just as fraud loss and leakage expose a firm to various losses, victims of identity theft typically incur both out-of-pocket losses and leakage costs. Out-of-pocket loss is the amount spent on recovery of the stolen identity such as lost wages or lengths of time and money spent on working with creditors and others to undo the wrongs and costs incurred due to the time needed to clean up the mess following theft such as lost wages from time off work or payment for services such as check verification and document replacement lost. And a leakage cost of identity theft is the theft itself cost such as higher credit charges or denial of credit due to the lower credit rating of the victim.

When an identity theft case arises, the victim can recover the out-of-pocket loss from the first-party insurance provider, who will get a new identity for the victim. The provider will help work with creditors to achieve a debt-free status for the victim by asking creditors to forgive any such debts. Thereafter, the insurer pays the deductible from the first-party insurance of the victim. However, for a theft loss that is much larger than the deductible and that is recurrent, and especially when the victim's recoverable costs are underestimated, the victim may not need the help of the first-person insurer. The victim deals directly with the thieves rather than the first-party insurers, and all these cases are usually managed by third-party insurers who provide liability coverage for firms that inadvertently fuel the crime.

9.7. Conclusion

Identity theft can include everything from stealing a person’s Social Security Number and altering news articles under their name to scamming money in a violated person’s name, saying inflammatory things while logged in to social media, or creating fake accounts on social media in a person’s name. And major organizations use our personal information for profit, but for how much longer? Could they be held accountable for leaking our information when they become liable for losses because of negligence? Are their policies really that protective or just a lock on a rotting door? Insurance products that help people monitor their cyber activity and alert them to potential danger when

companies use or sell information without consent, or negligent security practices are on the way.

Amidst all the concern over identity theft and compromised passwords and data security breaches at large corporations, it is easy to forget about the potential dangers of being a parent in a hyper-connected world. Technology nowadays allows almost limitless access to places like schools, daycare centers, and children's events where kids are present. In turn, it also makes it possible for the worst offenders to exploit that access. Although the risks of identity theft may be increasing, it does not mean you should stop using technology altogether. Cyber monitoring and protection insurance can help protect consumers from identity theft, as well as individuals who work in the employment of caring for their children.

9.7.1. Future Trends

In the context of the Future of Jobs Report, we are now more connected than ever before. People are living their lives online, relying on technology for work, shopping, leisure, and social interactions; at the same time, sensitive personal information is being collected and stored on potentially insecure networks and systems. With increasing interconnectivity comes an uptick in both the quantity and the sophistication of cyberattacks; cybercriminals are constantly devising new ways to exploit the vulnerabilities that inevitably arise in the online world. This confluence is leading to a variety of trends that will shape the future of identity theft risk and insurance.

For one, there is an increase in the monetization of cybercrime, leading to a corresponding growth in the popularity and severity of attacks, at least in the short to medium term. Organizations are investing in defenses, which is making attacks more costly and less successful, but increasing the costs for those that actually do decide to take the plunge. As new technologies like 5G, machine learning and artificial intelligence, and augmented reality become more prevalent, there will be an overall increase in the volume and sophistication of attacks in the short to medium term.

Cybercrime is evolving as it grows. Ransomware attacks are typically committed by organized criminal groups and are using ever more advanced tactics. In addition, cybercriminals are increasingly leveraging human weakness; attackers are regularly launching generalized social engineered attacks via email, phone, or text messaging to commit fraud. It appears that, while data is still being exfiltrated, ransomware attacks now frequently come after technology companies have invested in defenses against ransomware. While in the past cybercriminals would lock companies out of their systems and demand payment, with these so-called double-extortion schemes cybercriminals now also threaten to release sensitive data.

References

Englezos, E. (2022). # Hyperconnected: Law and the digital influence over individual identity.

Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. Technology in Society, 67, 101734.

Ghadge, M. N. (2024). Digital identity in the age of cybersecurity: Challenges and solutions. London Journal Of Research In Computer Science And Technology, 24(1), 1-10.

George, A. S. (2025). The Critical Role of Cybersecurity Insurance in an Era of Exponential Threats: A Review of Emerging Risk Realities and Policy Safeguards for Enterprise Resilience. Partners Universal International Research Journal, 4(1), 1-23.

Weippl, E., & Schrittwieser, S. (2024). Introduction to Security and Privacy. Hannes Werthner· Carlo Ghezzi· Jeff Kramer· Julian Nida-Rümelin· Bashar Nuseibeh· Erich Prem·, 397.

Shah, R. (2022). The future of digital identity in Australia. Australian Strategic Policy Institute.