ALLIEDUNIVERSAL®
RISK ADVISORY AND CONSULTING SERVICES
There for you.

IMPACT OF CRIME ON THE RETAIL INDUSTRY

• • • SPECIAL INTELLIGENCE REPORT - CRIME • • •

TABLE OF CONTENTS

INTELLIGENCE REPORT CONTRIBUTORS

Allied Universal® Risk Advisory and Consulting Services

- Marielle Dewicki – Intelligence Analyst
- Ahana Kowdley – Intelligence Analyst
- Brent Barnhill – Senior Intelligence Analyst

EXECUTIVE SUMMARY

The retail sector experiences a broad, often interconnected array of crime risks, many of which appear to be increasing in severity and frequency. Cybercrime, fraud, insider threats, organized crime, supply chain crime, theft, and violent crime (particularly involving guns) are among retailers' most significant, persistent, and rising threats worldwide. As in previous years, these crimes are anticipated to increase in frequency and severity over the next year. Crimes against retailers are likely to threaten business continuity and financial assets through reduced employee retention, investigations, lawsuits, loss of assets, damage to assets and facilities, and decreased customer and investor bases. As in the past, crime levels (along with potential negative effects on businesses) will almost certainly become heightened during significant shopping and sales events and holiday seasons, particularly from Black Friday through Cyber Monday in the U.S. and other countries participating in such retail events. The number and impact level of crimes against retailers over the next year will be heavily dependent on a variety of factors, including in-store and online security of retailers and their supply chains and the state of the global economy. However, retail corporations must strike an effective balance between security measures and customer shopping experience and efficiency, the latter of which is expected to continue to win out over the implementation of stronger anti-crime policies, as retailers will likely continue to prioritize financial gain from sales over the reduction in potential financial losses (and other negative effects) from crime.

ASSESSMENT

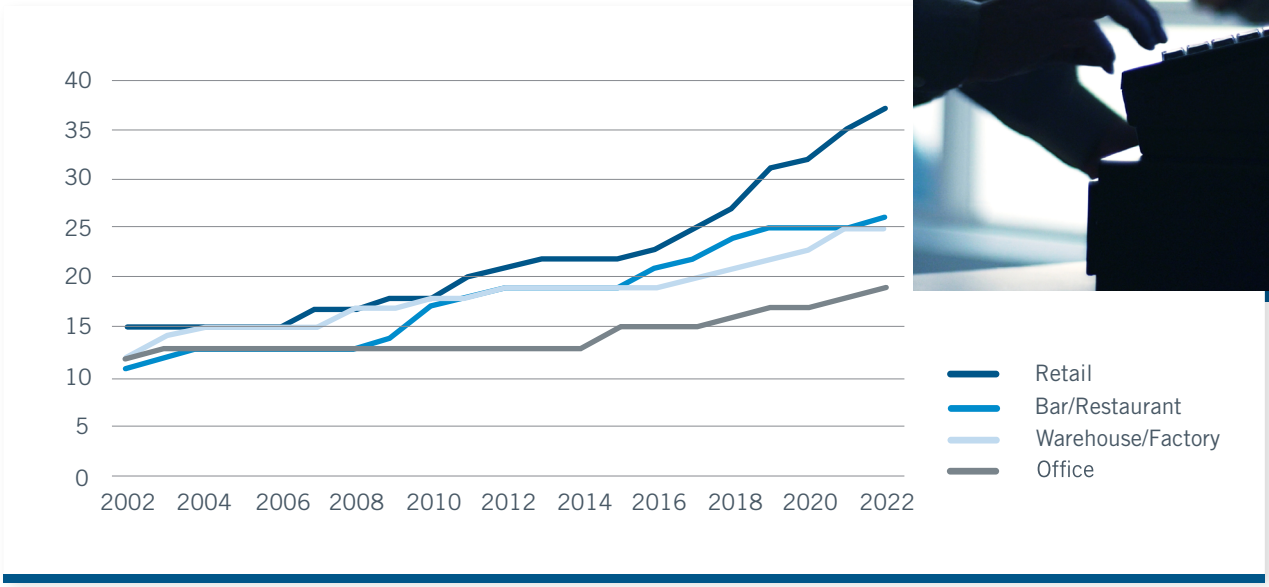
THEFT

Theft is a constant threat to online, physical stores, and omnichannel retailers and will likely continue to rise over the next year due in part to global economic challenges. Both employees and customers commit theft against retailers, sometimes in coordination with organized retail crime (ORC) gangs. Theft can occur in both physical stores and during product shipment (including at delivery locations), affecting online and omnichannel retailers as well. The COVID-19 pandemic led to a surge in theft against online retail businesses, as physical stores closed and customers increasingly shopped online, with products stolen during processing, shipment, and after delivery. These forms of theft have not declined since the reopening of physical stores, and the reopening process has led to in-store theft occurring more often. In the National Retail Federation's (NRF's) 2022 Retail Security Survey (covering 2021 data), 74.1% of respondents indicated that external theft (excluding ORC) poses an increasing risk and has become a more significant threat priority between 2016 to 2021, while 70.7% of retailers surveyed responded the same for ORC and 56.9% for internal theft. Since around 2020, in-store theft incidents, particularly those committed by ORC groups, have also become increasingly prone to forms of violence that include smash-and-grab, the use of firearms or other weaponry, battery, flash mob tactics, or threats of violence against store employees or customers. According to the NRF's 2023 Organized Retail Crime Report, an analysis of 132 gangs that conducted theft operations in the U.S. between 2014 and 2022 found that 16% of the groups used at least one violent tactic, and 15 out of the identified 21 violent ORC gangs began operating in 2021. These statistics indicate an uptick in violent theft. Selective reporting by the media may also skew public perception of violent retail theft, making the issue appear worse than it is, though violence has still likely become at least slightly more common during retail theft incidents in recent years. As the global economy worsens and moves towards a recession – and as inflation rises – over the next year, rising costs of necessary products are anticipated to heighten the frequency of violent and nonviolent theft incidents committed by customers, employees, and ORC groups against e-commerce, physical locations, and omnichannel retail companies. Store security and theft policies are almost certain to contribute to the rising number of theft cases, particularly ORC, as thieves tend to steal easily accessible (not locked) items that are popular with consumers, and locking up such items would inconvenience both employees and shoppers. Local theft legislation and penalties, unless they are tightened by lawmakers, are also likely to facilitate heightened retail theft (ORC). Penalties for nonviolent/petty theft may only be classified as a misdemeanor and punishable by a fine of several hundred dollars which, in comparison with the potential payoff from ORC, is unlikely to deter criminals. A higher number of theft incidents would almost certainly lead to greater financial losses for retailers caused by product theft, damage to stores and items, and operational disruption during the recovery period from theft incidents. Reputational damage and fear among customers, investors, and current and potential future employees would also likely cause financial losses for retail stores affected by significant and/or violent theft incidents, as customers may become afraid to shop at affected locations, investors may reduce funding if retail security appears weak, current employees may become afraid to come into work and seek new job opportunities, and potential new hires may not apply to work at affected companies. Repeated theft incidents against the same store location or same company would very likely worsen the potential business interruption, reputational damage, and financial losses.

VIOLENT CRIME

As with many other forms of crime, limited physical security measures and the reopening of physical stores after pandemic lockdowns have contributed to a rise in violent crime against retail businesses. This growth is expected to continue over the next year, at least in the United States. Violent crime against retail encompasses a variety of incident types, including violent theft, verbal and written threats and harassment, assault, intentional property destruction, and gun violence, among other incidents. Employees (including managers and executives), customers, and other individuals all commit such crimes, which are triggered by dissatisfaction with retailers (due to wages, commodity prices, political views, and other reasons), mental health issues, disputes between individuals, and other causes. Despite a lack of physical stores, online retailers are not invulnerable, as violent theft, assaults, and other incidents can occur in company offices, distribution centers, and other locations. According to the NRF's 2022 Retail Security Survey, 77.6% of respondents listed guest-on-associate violence as an increased risk and threat priority, 57.9% listed mass violence / active assailants, 52.6% listed gun violence, and 48.3% listed associate-on-associate violence in 2021. The number of mass shootings at U.S. retail stores, bars/restaurants, and warehouses/factories has more than doubled, and the number of mass shootings in offices has also risen in the past 20 years (see Figure 1), a trend which is anticipated to continue through the next year, if not longer. Retail stores world-wide are at particular risk of shootings, as businesses must balance physical security measures with customer satisfaction and ease of shopping, with the shopper experience often winning out over more stringent security measures that may aid in reducing the frequency and severity of shootings and other violent incidents. Beyond a growing number of casualties at stores, the growing number of mass shootings and other forms of violent retail crime increases the probability and potential severity of reputational damage, business disruption, and financial losses for retail companies. Businesses are sometimes blamed by shoppers and employees for facilitating these incidents as a result of allegedly weak security measures and may therefore experience lawsuits and protests. Retail stores and malls frequently remain closed for several days, weeks, or longer after shooting scenes are cleared, and even after the locations reopen, shoppers and employees are often wary of returning, thus heightening financial losses and operational disruption. Retailers who implement more stringent security measures may avert some of the short-term and long-term effects associated with violent crime. While concrete statistics on the benefits of the recent increase in armed security guards at retail businesses are not currently available, the rapid growth in retailers employing armed guards suggests a benefit, according to an article by Forbes. Armed security guards can help to reduce crime and its impacts more than video surveillance and other passive security measures, as they can respond immediately to potential incidences of theft, violence, and other issues – thus reducing possible facility damage, product losses, and human casualties – and their presence at store entrances may also help to dissuade would-be criminals and provide a sense of security for customers. However, the most effective security procedures are holistic and include multiple factors beyond the employment of armed guards, such as employee response training, canines, video surveillance, metal detectors, and other measures.

Figure 1: Number of U.S. Public Mass Shootings by Location, 2002 – 2022



Source: The Violence Project

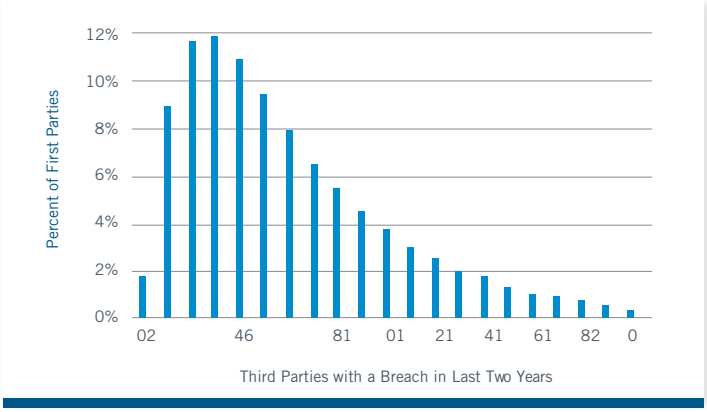
CYBERCRIME

As with many other sectors, cybercrime poses a continuous and growing threat to the global retail industry. In the NRF's 2022 Retail Security Survey. 58.6% of retail entities surveyed responded that their businesses experienced a growth in cybercrime risk and threat priority over the past five years – 43.15% of these respondents stated that the risk and threat priority increased "somewhat more," while 15.5% replied that these issues rose "much more." Of the threats listed in the report, cybercrime ranked as the fourth most significant in terms of the percentage of respondents that experienced a growth in threat categories. Retail organizations are increasingly susceptible to cybercrime due to weaker cybersecurity in stores, the close link between companies' physical stores and online platforms, growing reliance on Internet of Things devices, popularization of shadow IT, and prioritization of service speed over security. These vulnerabilities lead to diverse cybersecurity threats, including ransomware; credential spoofing, stuffing, and theft; and cybercriminal automation (using bots for online retail fraud), all of which will likely continue to rise in the long term for businesses worldwide. Credential stuffing is anticipated to become particularly problematic for retailers with e-commerce operations over the next year due to the size of their customer bases and the relative lack of user oversight of their accounts. The cybersecurity research firm Darktrace has reported that credential theft, spoofing, and stuffing were responsible for 170% more cybercrime incidents in the United States, 14% more in the United Kingdom, and 70% more incidents in Australia in 2022 than in the previous year. Despite an apparent 21% decline in global ransomware volume in 2022, ransomware will also still likely remain a pervasive threat to retailers, as a report by SonicWall found that e-commerce and online retail companies experienced a 264% growth in ransomware attacks between 2021 and 2022.

Third and fourth-party supply chain affiliates also provide a significant source of cybersecurity risk for retailers, particularly affiliates based in low-income countries and others with weak cybersecurity infrastructure and education, as attacks on these organizations can lead to leaked data and other threats for first-party organizations (see Figures 2 and 3). As with most industries, the retail sector will likely continue to struggle to respond to cybersecurity threats in the short and long term. The impacts of cybersecurity threats on retailers will remain as diverse and potentially significant as the threats themselves and extend beyond the organizations, including reputational damage, customer and investor losses, government investigations, lawsuits, employee retention and hiring difficulties, and financial losses. However, initiatives by individual companies, retail groups, and governments, such as strategic multilateral partnerships and increased cybersecurity budgets, could help to somewhat reduce the volume and severity of cyber threats and their impacts in the long term.

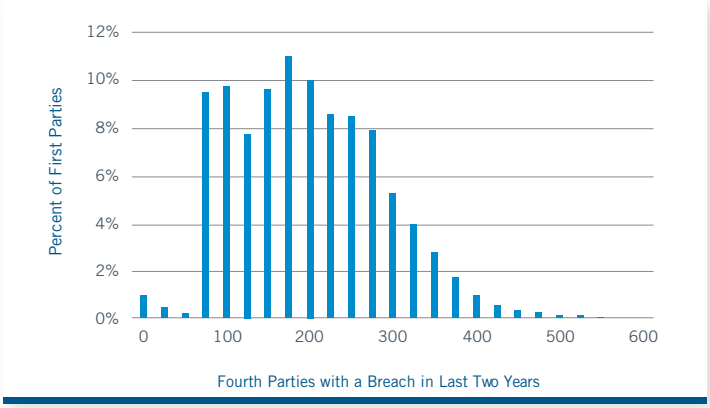
The NRF has also partnered with the Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC) to tackle malicious cyberattacks and heighten the protection of customer data. However, the program's effectiveness will depend on the quality of participation by the organizations and their subscribers and the industry responses to the shared information. The recently released CISO Benchmark Report also found that approximately 70% of CEOs surveyed in the retail and hospitality sector anticipate cybersecurity budget and personnel increases in 2023, which (assuming the efficacy of corporations' cybersecurity programs) could at least slightly diminish cybersecurity risks for those companies.

Figure 2: First Parties with Compromised Third Parties in the Last Two Years



Source: Cyentia Institute and SecurityScorecard

Figure 3: First Parties with Compromised Fourth Parties in the Last Two Years



Source: Cyentia Institute and SecurityScorecard

ORGANIZED CRIME

Organized crime threats against the retail industry will likely increase over the next year, with the potential to incur widespread asset and financial losses as well as reputational damage due to a perceived lack of security, delayed shipments, stolen purchases, and damaged goods. The National Retail Federation reported that organized retail crime (ORC) accounted for nearly half of the $94.5 billion in shrink (loss) of physical inventory in 2021, and the overall shrink rate from 2016 to 2021 remained at 1.4% of annual sales. Organized crime threats include a broad range of risks, including impersonation of companies and corporate actors, cargo theft, and cybercrime through fraudulent order submissions and transportation requests. ORC groups range in size from a few individuals to complex enterprises with established organized hierarchies and primarily target everyday consumer goods, like electronics, focusing on items outlined in the CRAVED model (items that are Concealable, Removable, Available, Valuable, Enjoyable, and Disposable). These are products that are concealable, removable, available, valuable, enjoyable, and disposable, and they are targeted because they require minimal time and effort to gain access to, minimize the risk of negative consequences, and maximize the benefits of a given offense. According to the 2022 National Retail Security Survey (NRSS), over 70% of surveyed retailers stated that combatting ORC is an increasingly higher priority for their organizations, with many establishing dedicated teams to the mitigation of retail crime risk. Cargo theft by ORC groups is the most prominent risk posed by organized crime against the retail industry, particularly during the loading and unloading of goods in ports, rail hubs, truck stops, warehouses, and other transitional areas along the supply chain where cargo remains stationary for large periods of time. The 2022 NRSS additionally stated that in FY 2021, external theft, including ORC, contributed to nearly 37% of all inventory loss, and the COVID-19 pandemic was a major contributor to the increase in ORC, with a reported risk increase of nearly 71%, due to port lockdowns, strict quarantine guidelines, and disruptions to the global supply chain which kept cargo stationary for extended periods of time. While the strain on the supply chain has decreased since the relaxation of pandemic guidelines, ORC groups continue to threaten the retail industry.

Aggression and violence associated with ORC groups is another major industry concern, with nearly 82% of the 2022 NRSS respondents reporting that ORC offenders are somewhat more or much more violent when compared to the previous year and 35.9% reporting ORC offenders as much more violent when compared to the previous year. With violence against the retail industry expected to increase, the potential risk to employees along the supply and distribution chains is high, and employers will need to take precautions to protect employees' physical safety. In addition to violence, ORC groups have increased criminal impersonations of legitimate companies to facilitate the theft of trucking loads, cargo, and merchandise. These groups also impersonate carriers to respond to online job bids that involve the loading and delivery of goods or submit fraudulent orders and transportation requests to gain access to cargo shipments and steal inventory. Each of these activities contributes to inventory shortages, delayed shipments, financial losses, and reputational damage to retail corporations. Repeated cargo theft incidents against the same companies, industries, or cargo facilities and transportation hubs would likely worsen potential business interruption, reputational damage, and financial losses.

FRAUD

Fraud in the physical world and online presents a growing threat to retailers. Despite efforts to combat this form of crime, it will likely occur with increasing frequency (if not severity) over the next year. The retail industry faces several forms of fraud, including counterfeit product creation and sales, order claim fraud, gift card fraud, audit fraud, credential fraud, and buy-now-pay-later fraud. In the NRF's 2022 Retail Security Survey, 69% of respondents stated that in-store fraud rose, 61.1% indicated that e-commerce fraud increased, and 53.9% responded that omnichannel fraud grew in 2021, with respondents listing gift card fraud, coupon/discount/loyalty fraud, return fraud, and payment (card/check) fraud among the top twelve crimes that increased in risk and priority over the past five years. A significant portion of the rise in fraud, particularly counterfeit (and potentially faulty and dangerous) items such as medical products and medicines (which was already highly problematic pre-pandemic), is attributed to the COVID-19 pandemic, which led to a surge in demand for health-related products, supply chain shortages for those items, and a decline of government and business oversight of fraud. The pandemic-caused growth in e-commerce also led to a surge in e-commerce fraud (over in-store fraud), though in-store fraud has largely rebounded and is expected to continue to rise as the pandemic ends and shoppers return to physical stores. E-commerce fraud will also likely continue to rise over the next year, as will the production and sale of counterfeit items, though likely not at the surging rates experienced during the pandemic.

The drop in pandemic-era supply chain shortages, along with recent company initiatives (such as Amazon's Counterfeit Crimes Unit and Insurance Accelerator) and government legislation (such as the U.S. INFORM Consumers Act) to address the sale of illicit and counterfeit products, may help to at least slightly moderate omnichannel retail fraud and the sale of counterfeit and potentially dangerous items on popular e-commerce websites. However, any potential benefits would not likely become visible in the short term (over the next few months), and the efficacy of these efforts would depend on their enforcement and budgets, among other factors. As with anti-fraud efforts in the past, the retail industry's need to prioritize customer experience and shopping efficiency over addressing fraud may somewhat reduce the potential benefits of anti-fraud measures. These initiatives also do little to identify and prosecute individuals committing fraudulent acts, which is frequently hindered by online criminals' ability to hide and change their identities and the fact that they may be located in foreign countries. This allows many fraudsters to continue their activities and renders anti-fraud efforts more reactive than proactive, reducing their effectiveness. Furthermore, though countries such as the U.S. maintain well-established laws and investigation processes to identify and prosecute internal corporate fraud (committed by employees, investors, executives, and others within a company), retailers remain susceptible to illegal audit modifications, bribery, and other forms of fraud. Regardless of whether a fraud incident against a retail business is committed by internal or external actors (or both), reputational damage and financial losses – whether caused directly by the actions of fraudsters or as a result of a potentially reduced customer or investor base – are almost guaranteed. Investigations by government and business entities, along with potential lawsuits and penalties (including fines), are possible, particularly in the instance of significant financial losses, internal (company) complicity, and injury or financial loss to customers (particularly resulting from the purchase of counterfeit goods). Employee retention and replacement may also become difficult following fraud incidents involving internal collusion or in which employees are negatively affected (through financial losses, stolen credentials, or other impacts).

SUPPLY CHAIN CRIME

Supply chain crime, particularly cargo theft, will likely occur more frequently in the coming year than in previous years, with the potential to incur greater asset and financial losses. Retail supply chains contain a number of vulnerable nodes, including factories, distribution centers, and local stores, which are prone to theft, fraud, cybercrime, and other crimes by individuals internal and external to the supply chain. Cargo theft by organized crime groups presents an especially problematic crime risk to retailers worldwide, particularly in ports, rail hubs, truck stops, warehouses, and other locations in which cargo remains stationary during transport. Cargo theft incidents rose by 84% between 2019 and 2021 in the U.S. and Canada, according to the NRF's 2023 Organized Retail Crime Report. The increase in theft is partially due to global supply chain issues triggered by COVID-19 lockdowns. This created a high demand for items in short supply and left many goods idle in transit locations, allowing products to be stolen and sold online and in physical stores through third-party sellers and disreputable vendors. Some of these sellers and vendors may have then laundered their profits. The COVID-19 supply chain shortage also heightened supply chain fraud, including counterfeiting operations (particularly of medical supplies and medicines) and price gouging by retailers, threatening the health and purchasing power of consumers, causing financial losses for companies, and leading to reputational damage for some companies accused of taking advantage of supply shortages. Though pandemic-era supply chain shortages and disruptions have abated, supply chain theft (including cargo theft), fraud, and cybercrime by organized crime groups continue to rise. Global inflation growth, along with an anticipated recession, will likely continue to increase the frequency and severity of supply chain crime and resulting financial losses as consumers struggle to cope with rising retail prices, and some (including retail and shipping employees) turn to crime or to online or physical third-party sellers (including counterfeiters) to acquire goods. Heightened crime against retail supply chains may also result in increased reputational damage to retailers due to perceptions of weak retailer security or a lack of customer care caused by delayed product shipments, stolen purchases (such as incidents of porch piracy), destroyed or damaged goods, and item shortages.

While supply chain crime traditionally encompasses incidents such as theft, fraud, and cybercrime against involved businesses, this classification also includes regulatory noncompliance (both intentional and unintentional), such as sanctions, environmental law, and human rights violations committed by companies in a supply chain. These legal violations may damage a retailer's reputation, disrupt operations, and threaten revenue as much as theft, fraud, and cybercrime. Tightening government restrictions and growing public concern surrounding business and supply chain practices mean that retailers must heighten their due diligence efforts across their supply chains and potentially divest from partner entities in order to reduce the possibility of legal violations, reputational damage, investigations, lawsuits, penalties, protests, and boycotting efforts, all of which frequently result in financial losses. However, compliance and supply chain restructuring measures are also costly and may result in heightened consumer costs. The latter of which threaten businesses' consumer and investor bases. Retailers must weigh the benefits and risks of strict regulatory and environmental social governance practices versus satisfying customers and maintaining low production and consumer costs. Russia's invasion of Ukraine and heightened Western concerns over China's human rights practices have added extra compliance complications over the past few years, as the U.S., Europe, and other governments have continuously levied new sanctions against Russian, Chinese, and other entities. Retailer companies have been particularly affected by U.S. sanctions affiliated with China's Xinjiang region, as multiple clothing retailers and others in the industry use manufacturers located in Xinjiang, due to fairly cheap production costs, and some businesses must now divest from those suppliers or risk government prosecution for violations and reputational damage, along with a potential reduction in customers and investors and likely financial losses. This divestment means that companies may now need to seek suppliers with potentially higher production costs, meaning customers may need to pay higher prices for goods at a time when the global economy is at risk of recession. These higher prices, as stated in the previous paragraph, increase the likelihood of customers turning to theft or third-party retail sellers (including counterfeiters), which would increase financial losses for companies. The current geopolitical and economic events will likely continue to strain retailers' compliance efforts and cost-cutting measures over the next year as they determine their operational priorities, and at least minor financial losses are possible no matter how companies choose to proceed.

INSIDER THREATS

Insider threats will almost certainly remain a persistent, although not necessarily increasing crime risk to the retail industry over the next year. As with other forms of crime, insider threats encompass a broad range of physical security, cybersecurity, and other risks mentioned separately in this report, such as online and in-person fraud, theft, verbal and physical harassment, and assault of coworkers and customers. Of the twelve crime types listed in the 2022 Retail Security Survey by the NRF, internal theft, and associate-on-associate violence were both listed as presenting an increase in risk and priority from 2016 to 2021; 56.9% of respondents identified internal theft, while 48.3% identified associate-on-associate violence as rising threats and business priorities. Internal theft and fraud can arise from financial motivations, disgruntled employees, and other factors and may sometimes be undertaken in connection with organized retail crime groups. Associate-on-associate violence, including harassment and assault, may result from employee disagreements, mental illness, or other reasons. Several major violent incidents involving employees have occurred in the past year, including a mass shooting by an employee of a multinational big box retailer and sexual harassment and assault cases allegedly committed by a CEO of a U.S.-based clothing retailer. Employees of all levels, from cashiers to managers to CEOs, have committed, been accused of, or been convicted of assault and other crimes. With the rise of the “Me Too” movement and growing customer interest in corporate environmental social governance programs (including environmental and labor law violations), the C-suite and other high-level employees are increasingly likely to be investigated and prosecuted for crimes when such incidents may have been largely ignored or never publicized even ten years ago. Sexual crimes and other legal violations, as with all other forms of insider crime threats, are highly likely to damage retailers’ reputations and may lead to calls by the public and investors for boycotts, potentially across multiple brands (for retail conglomerates). Financial losses are also certain to occur in internal theft cases, along with potential damage to other assets when violent organized crime groups are involved. Retailers may also incur losses from insider threats that lead to investigations (both internal and external) and lawsuits resulting from incidents involving injuries or threats toward or caused by employees, as well as accusations of law violations and demonstrations by employees and members of the public. Insider threats of all types, particularly when publicized and when employees are negatively impacted, are also likely to reduce employee retention and increase replacement costs, at least temporarily.

METHODOLOGY

Allied Universal® Risk Advisory and Consulting Services uses collection of intelligence and information, validation of all information received, and analysis of the impact of that information to present the client with an overall security risk assessment. Our intelligence analysts reviewed crime statistical data, mapping tools, academic literature, and security assessments from U.S. government sources, press, academia, and intelligence sources.

The information cut-off date for this report is June 30, 2023, unless otherwise stated within a section of the report.

COLLECTION AND VALIDATION

The intelligence analysts at Allied Universal rely on a variety of source information in their initial assessment of a client's risk exposure. Analysts examine open-source information, including government sites, social media, the press, and academia. Unlike other companies, our analysts have access to in-country human sources and in-country security officers who can provide information and collect intelligence from local sources, such as police, security forces, government officials, and journalists.

ANALYSIS

Good analysts know that not everything that is in the news or social media will impact the overall security risk. Allied Universal analysts are able to sift through all the "noise" by using different analytical and validation tools to determine events likely to impact the overall security environment. Information is sorted by its reliability, its immediate impact, and its potential to impact the security environment. Security risks can be further broken down by type and area to accommodate the client's specific concerns.

INTELLIGENCE SERVICES

Research and Analysis Allied Universal® is a one-stop shop for comprehensive intelligence risk assessments to help clients understand their ever-changing risk landscape. Our all-encompassing, bespoke reporting provides an in-depth review—from physical security for assets to reputational security threats identified across social media, deep web, and media outlets. These holistic assessments can be tailored to focus on risks to companies, events, individuals, locations, or travel plans. Services include comprehensive reports covering near-term and long-term security concerns.

Threat Monitoring Our intelligence analysts utilize advanced technology solutions to actively monitor the surface, deep, and dark web to report on identified threats. These solutions support fixed-asset locations, proactive traveler monitoring and alerting, emergency mass notifications, and multiple levels of reporting cadences, based on client requirements. We tailor threat monitoring and reporting for specific requirements, focusing on threats to a client's critical infrastructure (people, facilities and assets, business operations, and reputation), an event, or for a specific individual or topic.

Travel Risk Management A full suite of services are available to fulfill an organization's duty of care concerns for both domestic and international travel. Services include a host of intelligence products to assist in identifying and mitigating risks before and during travel. Pre-trip briefings prepare travelers for risks they might encounter and offer resources to manage any potential emergency situations. On-going situational monitoring and reporting assist travelers in staying appraised of local developments and potentially impactful events. Critical information can be passed via emergent reporting to ensure travelers avoid potential hazards, and risks can be further mitigated by traveler tracking services, allowing for immediate responsiveness to standard and emergent situations.

Consulting and Training Allied Universal subject matter experts provide a full range of intelligence consulting services for intelligence programs, security operations centers, and verbal or in-person briefing on security topics. We offer training and mentorship options, tailored to client needs, led by intelligence experts with industry, government, and military experience. Our scalable training solutions include on-demand, pre-recorded training sessions and in-person instruction from single sessions to develop and improve knowledge on a specific sector, topic, or skillset, to bespoke, interactive, and engaging training programs to elevate a client's entire intelligence department or GSOC capabilities. Bespoke options include the review of intelligence programs to ensure that training is focused on areas requiring improvements.

Intelligence Analysts Whether an organization requires an entire intelligence team, a single full-time analyst to support operations in-person, or part-time remote support, our team can provide this support. Allied Universal's successful embedded intelligence analyst program has provided our client's with experienced, reliable, professionals based on their specific requirements. We help ensure the long-term success of our analysts through continued engagement and support tailored to needs. This support ranges from personalized reviews and collaboration to set-up product lines andservices, to ongoing training and development. Our embedded analysts supporting clients have automatic access to ongoing training for career development and continuous improvement in the services they provide.

Technology Solutions We work with clients to provide the best technology solutions to meet their intelligence requirements and increase their effectiveness. Our team continually evaluates current and emerging technology to help support client's intelligence programs and wider security operations. We can assist with the implementation of the technology platforms and provide an extra layer of support, advocating for clients' needs. For clients needing a global view, our online monitoring Global Intelligence System (GIS) delivers geopolitical intelligence on current and future threats to corporate security, travel, and business continuity.

ALLIED UNIVERSAL®
RISK ADVISORY AND CONSULTING SERVICES
There for you.

TO LEARN MORE
www.aus.com