Form 8-K, Item 1.05 - Historical Filings

Issuer	Filing Date	Link to EDGAR Filing	Date of Amendment	Link to EDGAR Filing (Amendments)	Date of Comment Letter	Link to EDGAR Filing (Comment Letters)	Summary
V.F. Corporation (VFC)	12/15/2023	https://www.sec.gov/ix?doc=/Archives/edgar/data/103379/000095012323011228/d659095d8k.htm	1/18/2024	https://www.sec.gov/Archives/edgar/data/103379/000119312524010243/d641969d8ka.htm	1/5/2024	https://www.sec.gov/Archives/edgar/data/0000103379/000000000024000221/filename1.pdf	V.F. Corporation disclosed that a threat actor encrypted certain IT systems and exfiltrated data, including personal data, resulting in operational disruptions that impacted order fulfillment and business operations while retail stores and e-commerce sites remained largely operational. The company stated the incident has had and is reasonably likely to continue to have a material impact on business operations, and has not yet determined whether it is reasonably likely to materially impact its financial condition or results of operations.
First American Financial Corporation (FAF)	12/22/2023	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001472787/000095017023072513/faf-20231220.htm	12/29/2023	https://www.sec.gov/ix?doc=/Archives/edgar/data/1472787/000095017023073848/faf-20231220.htm	1/23/2024	https://www.sec.gov/Archives/edgar/data/1472787/000000000024000923/filename1.pdf	First American disclosed that it identified unauthorized activity on certain of its IT systems and took steps to contain, assess, and remediate the incident, including isolating systems from the Internet. The company stated that the disruption may render its primary website inaccessible, restoration timing is unknown, and it has not yet determined whether the incident may have a material impact on its financial condition or results of operations.
			1/12/2024	https://www.sec.gov/Archives/edgar/data/1472787/000095017024004247/faf-20231220.htm			
Microsoft Corporation (MSFT)	1/19/2024	https://www.sec.gov/Archives/edgar/data/789019/000119312524011295/d708866d8k.htm	3/8/2024	https://www.sec.gov/Archives/edgar/data/789019/000119312524062997/d808756d8ka.htm	6/17/2024	https://www.sec.gov/Archives/edgar/data/789019/000000000024006936/filename1.pdf	Microsoft disclosed that a nation-state associated threat actor gained unauthorized access to and exfiltrated information from a very small percentage of employee email accounts, including those of senior leadership and employees in cybersecurity, legal, and other functions, beginning in late November 2023. The company stated it removed the threat actor's access, the incident has not had a material impact on operations, and it has not yet determined whether the incident is reasonably likely to materially impact its financial condition or results of operations.
Hewlett Packard Enterprise Company (HPE)	1/24/2024	https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/1645590/000164559024000009/hpe-20240119.htm	N/A	N/A	6/4/2024	https://www.sec.gov/Archives/edgar/data/1645590/000000000024006387/filename1.pdf	Hewlett Packard Enterprise disclosed that a suspected nation-state actor gained unauthorized access to its cloud-based email environment and exfiltrated data from a small percentage of mailboxes beginning in May 2023, including those belonging to personnel in cybersecurity and other business functions. The company stated the incident has not had a material impact on its operations and has not determined that it is reasonably likely to materially impact its financial condition or results of operations.
SouthState Corporation (SSB)	2/9/2024	https://www.sec.gov/Archives/edgar/data/764038/000095010324002017/dp206600_8k.htm	3/29/2024	https://www.sec.gov/Archives/edgar/data/764038/000155837024004390/ssb-20240206x8ka.htm	5/31/2024	https://www.sec.gov/Archives/edgar/data/764038/000000000024006278/filename1.pdf	SouthState disclosed that it detected a cybersecurity incident and took measures to isolate parts of its network and disrupt unauthorized activity, resulting in some disruption to business processes while operations continued in all material respects. The company stated the incident has not had a material impact on operations and has not been determined to be reasonably likely to materially impact its financial condition or results of operations.
Prudential Financial, Inc. (PRU)	2/13/2024	https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/1137774/000119312524033753/d770643d8k.htm	2/21/2024	https://www.sec.gov/Archives/edgar/data/1137774/000119312524040749/d766318d8ka.htm	6/7/2024	https://www.sec.gov/Archives/edgar/data/1137774/000000000024006599/filename1.pdf	Prudential disclosed that a threat actor gained unauthorized access to certain of its IT systems and accessed Company administrative and user data, including a small percentage of user accounts associated with employees and contractors. The company stated it has no evidence that customer or client data was taken, and that the incident has not had a material impact on operations and has not been determined to be reasonably likely to materially impact its financial condition or results of operations.
UnitedHealth Group Inc (UNH)	2/22/2024	https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm	3/8/2024	https://www.sec.gov/Archives/edgar/data/731766/000073176624000085/unh-20240221.htm	6/4/2024	https://www.sec.gov/Archives/edgar/data/731766/000000000024006401/filename1.pdf	UnitedHealth disclosed that a suspected nation-state associated threat actor gained access to certain Change Healthcare IT systems, prompting the company to isolate affected systems and resulting in disruption to certain networks and transactional services. The company stated other systems remained operational and has not determined that the incident is reasonably likely to materially impact its financial condition or results of operations.
			4/24/2024	https://www.sec.gov/Archives/edgar/data/731766/000073176624000085/unh-20240221.htm			
Cencora, Inc. (COR)	2/27/2024	https://www.sec.gov/Archives/edgar/data/1140859/000110465924028288/tm247267d1_8k.htm	7/31/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/1140859/000110465924084351/tm2420501d1_8ka.htm	6/6/2024	https://www.sec.gov/Archives/edgar/data/1140859/000000000024006510/filename1.pdf	Cencora disclosed that data was exfiltrated from its information systems, some of which may contain personal information, and that it initiated containment measures and an investigation with law enforcement, cybersecurity experts, and external counsel. The company stated that the incident has not had a material impact on its operations and that its systems remain operational, and it has not yet determined whether the incident is reasonably likely to materially impact its financial condition or results of operations.

Form 8-K, Item 1.05 - Historical Filings

Issuer	Filing Date	Link to EDGAR Filing	Date of Amendment	Link to EDGAR Filing (Amendments)	Date of Comment Letter	Link to EDGAR Filing (Comment Letters)	Summary
Federal Home Loan Bank of New York	3/1/2024	https://www.sec.gov/Archives/edgar/data/1329842/000165495424002505/fhlbny_8k.htm	N/A	N/A	5/24/2024	https://www.sec.gov/Archives/edgar/data/1329842/000000000024006064/filename1.pdf	The Federal Home Loan Bank of New York disclosed that unknown persons attempted to fraudulently obtain funds through a compromise involving a fourth-party vendor, prompting the bank to activate its response process and take containment and remediation measures. The bank stated that its own systems were not compromised, no unauthorized transactions occurred, and the incident has not had and is not expected to materially impact its operations, financial condition, or results of operations.
MarineMax, Inc. (HZO)	3/12/2024	https://www.sec.gov/Archives/edgar/data/1057060/000095017024030041/hzo-20240310.htm	4/1/2024	https://www.sec.gov/Archives/edgar/data/1057060/000095017024038881/hzo-20240310.htm	6/3/2024	https://www.sec.gov/Archives/edgar/data/1057060/000000000024006350/filename1.pdf	MarineMax disclosed that a third party gained unauthorized access to portions of its information environment, and that containment measures resulted in some disruption to a portion of its business while operations continued in all material respects. The company stated the incident has not had a material impact on operations and is still determining whether it is reasonably likely to materially impact its financial condition or results of operations.
Radiant Logistics, Inc. (RLGT)	3/20/2024	https://www.sec.gov/Archives/edgar/data/1171155/000095017024033954/rlgt-20240319.htm	N/A	N/A	6/4/2024	https://www.sec.gov/Archives/edgar/data/1171155/000000000024006371/filename1.pdf	Radiant disclosed that it detected a cybersecurity incident affecting its Canadian operations and took measures to isolate those operations and disrupt unauthorized activity, resulting in service delays for customers in Canada while recovery efforts are underway. The company stated its U.S. and other international operations continued without disruption, and the incident has not had a material impact on overall operations and has not been determined to be reasonably likely to materially impact its financial condition or results of operations.
B. Riley Financial, Inc. (RILY)	4/8/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001464790/000121390024031252/ea020350 0-8k_briley.htm	N/A	N/A	6/4/2024	https://www.sec.gov/Archives/edgar/data/1464790/000000000024006411/filename1.pdf	B. Riley disclosed that a threat actor gained unauthorized access to certain file systems of its indirect subsidiary, Targus International, LLC, prompting the activation of incident response and containment measures that resulted in a temporary interruption of Targus' business operations. The incident has been contained and system recovery efforts are ongoing, and while the disruption affected Targus operations, the company stated it does not currently believe the incident will materially impact its financial condition or results of operations.
OraSure Technologies, Inc. (OSUR)	4/12/2024	https://www.sec.gov/Archives/edgar/data/1116463/000119312524094797/d825009d8k.htm	N/A	N/A	5/24/2024	https://www.sec.gov/Archives/edgar/data/1116463/000000000024006063/filename1.pdf	OraSure disclosed that an unauthorized third party gained access to company data from certain information systems and exfiltrated certain files, and that the company initiated response protocols, engaged external experts, and notified law enforcement. The company stated the incident has not had a material impact on its operations, financial systems, or financial condition, and does not anticipate a material impact on its financial condition or results of operations.
Frontier Communications Parent, Inc. (FYBR)	4/18/2024	https://www.sec.gov/Archives/edgar/data/20520/000119312524100764/d784189d8k.htm	N/A	N/A	6/4/2024	https://www.sec.gov/Archives/edgar/data/20520/000000000024006370/filename1.pdf	Frontier disclosed that a third party gained unauthorized access to portions of its IT environment, including personally identifiable information, and that containment measures such as shutting down certain systems resulted in an operational disruption that could be considered material. The company stated it has contained the incident and is restoring normal operations, and does not believe the incident is reasonably likely to materially impact its financial condition or results of operations.
Dropbox, Inc. (DBX)	5/1/2024	https://www.sec.gov/Archives/edgar/data/1467623/000146762324000024/dbx-20240429.htm	N/A	N/A	6/3/2024	https://www.sec.gov/Archives/edgar/data/1467623/000000000024006355/filename1.pdf	Dropbox disclosed that a threat actor gained unauthorized access to the Dropbox Sign production environment and accessed user data, including emails, usernames, account settings, and for some users, phone numbers, hashed passwords, and authentication information such as API keys and tokens. The company stated there is no evidence that the contents of user accounts or payment information were accessed and that the incident has not had, and is not reasonably likely to have, a material impact on its business operations, financial condition, or results of operations.
Brandywine Realty Trust (BDN)	5/7/2024	https://www.sec.gov/Archives/edgar/data/1060386/000119312524133132/d824906d8k.htm	5/28/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000790816/000119312524147625/d774339d8ka.htm	6/10/2024	https://www.sec.gov/Archives/edgar/data/790816/000000000024006670/filename1.pdf	Brandywine disclosed that a third party gained unauthorized access to portions of its IT environment and deployed encryption on certain internal corporate systems, resulting in disruptions to and limited access to business applications supporting operations and corporate functions, including financial and operating reporting systems. The company also identified that certain files were exfiltrated and is investigating whether sensitive information was involved, and while the incident has been contained and operations have continued in all material respects, the company stated it does not believe the incident is reasonably likely to materially impact its financial condition or results of operations.

Form 8-K, Item 1.05 - Historical Filings

Issuer	Filing Date	Link to EDGAR Filing	Date of Amendment	Link to EDGAR Filing (Amendments)	Date of Comment Letter	Link to EDGAR Filing (Comment Letters)	Summary
Key Tronic Corporation (KTCC)	5/10/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000719733/000071973324000015/ktcc-20240506.htm	6/14/2024 8/14/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/719733/000071973324000035/ktcc-20240506.htm https://www.sec.gov/ix?doc=/Archives/edgar/data/719733/000071973324000035/ktcc-20240506.htm	N/A	N/A	Key Tronic disclosed that an unauthorized third party accessed portions of its IT systems, resulting in disruptions and limited access to business applications supporting operations and corporate functions, including financial and operating reporting systems. The company stated the incident has been contained and it is working to restore affected systems, and does not believe the incident is reasonably likely to have a material impact on its financial condition or results of operations.
Sonic Automotive, Inc. (SAH)	7/5/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/1043509/000104350924000060/sah-20240705.htm	8/5/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/1043509/000104350924000063/sah-20240705.htm	N/A	N/A	Sonic Automotive disclosed that a cybersecurity incident affecting systems provided by CDK Global disrupted access to its dealer management, customer relationship management, and other systems supporting sales, inventory, and accounting functions, with some systems remaining offline and full restoration timing unclear. The company stated the incident is reasonably likely to have a material impact on its results of operations for the second fiscal quarter of 2024 due to reduced vehicle sales, while the broader financial impact has not yet been determined.
AT&T Inc. (T)	7/12/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000732717/000073271724000046/t-20240506.htm	N/A	N/A	45499	https://www.sec.gov/Archives/edgar/data/732717/000000000024008480/filename1.pdf	AT&T disclosed that threat actors unlawfully accessed an AT&T workspace on a third-party cloud platform and, between April 14 and April 25, 2024, exfiltrated files containing records of customer call and text interactions from specified 2022 and 2023 periods, affecting nearly all of its wireless customers and certain mobile virtual network operator customers. The data did not include call or text content or certain personal information, AT&T closed the point of access and is notifying impacted customers, and the company stated the incident has not had a material impact on its operations or is reasonably likely to materially impact its financial condition or results of operations.
Bassett Furniture Industries, Incorporated (BSET)	7/15/2024	https://www.sec.gov/Archives/edgar/data/10329/000143774924022743/bset20240715_8k.htm	8/6/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000010329/000143774924024679/bset20240805_8ka.htm	N/A	N/A	Bassett disclosed that a threat actor encrypted certain data files after unauthorized occurrences on a portion of its IT systems, leading the company to shut down some systems and resulting in disruption to business operations, including an inability to operate manufacturing facilities and impacts to order fulfillment. The company stated that personal information was not believed to be compromised, and while the full scope remains under investigation, the incident has had and is reasonably likely to continue to have a material impact on business operations, with the financial impact not yet determined.
Crimson Wine Group, LTD (CWGL)	7/25/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001562151/000156215124000032/cwgl-20240725.htm	N/A	N/A	N/A	N/A	Crimson Wine Group disclosed that an unauthorized third party gained access to a portion of its internal information systems and exfiltrated certain files, including files potentially containing sensitive personal information, and that the company shut down certain systems to isolate operations, resulting in business disruption and limited access to certain applications. The company determined that the incident has likely had a material impact on business operations, but stated it does not believe the incident has had or is reasonably likely to materially impact its financial condition or results of operations.
Meta Materials Inc. (MMAT)	8/1/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/1431959/000095017024089345/mmat-20240725.htm	N/A	N/A	N/A	N/A	Meta Materials disclosed that its website, email system, and other IT systems were disrupted and taken offline after a former executive officer deliberately deactivated and cancelled the website renewal, impacting communications and system functionality. The company stated systems were subsequently restored, is evaluating any unauthorized access to sensitive information, and has not yet determined whether the incident is reasonably likely to materially impact its financial condition or results of operations.
Halliburton Co (HAL)	9/3/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/45012/000004501224000052/hal-20240830.htm	N/A	N/A	45582	https://www.sec.gov/Archives/edgar/data/45012/000000000024011681/filename1.pdf	Halliburton disclosed that an unauthorized third party gained access to certain of its systems and exfiltrated information, prompting the company to take certain systems offline and resulting in disruptions and limited access to business applications supporting operations and corporate functions. The company stated it continues to provide products and services while restoring systems and assessing impacted data, and does not believe the incident has had or is reasonably likely to materially impact its financial condition or results of operations.

Form 8-K, Item 1.05 - Historical Filings

Issuer	Filing Date	Link to EDGAR Filing	Date of Amendment	Link to EDGAR Filing (Amendments)	Date of Comment Letter	Link to EDGAR Filing (Comment Letters)	Summary
iLearningEngines, Inc. (AILE)	11/18/2024	https://www.sec.gov/Archives/edgar/data/1835972/000121390024099394/ea0221424-8k_ilearning.htm	N/A	N/A	N/A	N/A	iLearningEngines disclosed that a threat actor accessed its environment and certain network files, misdirected a $250,000 wire payment that was not recovered, and deleted a number of email messages. The company stated the incident has been contained and is expected to have a material impact on operations for the quarter ended December 31, 2024, but is not expected to have a material impact on full year 2024 results.
ENGlobal Corporation (ENG)	12/2/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/933738/000165495424015098/eng_8k.htm	1/27/2025	https://www.sec.gov/Archives/edgar/data/933738/000165495425000798/eng_8ka.htm	N/A	N/A	ENGlobal disclosed that a threat actor illegally accessed its IT system and encrypted certain data files, prompting the company to initiate containment and remediation measures, including restricting access to its systems. As a result, access to the IT system has been limited to essential business operations, restoration timing remains unclear, and the company has not yet determined whether the incident is reasonably likely to materially impact its financial condition or results of operations.
Krispy Kreme, Inc. (DNUT)	12/11/2024	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001857154/000185715424000123/dnut-20241211.htm	N/A	N/A	N/A	N/A	Krispy Kreme disclosed that unauthorized activity on a portion of its IT systems disrupted operations, including its online ordering platform in parts of the United States, while retail locations and deliveries continued operating. The company stated the incident has had and is reasonably likely to have a material impact on business operations and is expected to materially impact its financial condition and results of operations due to lost digital sales and remediation costs.
Lee Enterprises, Inc. (LEE)	2/18/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000058361/000162828025005855/lee-20250212.htm	3/6/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000058361/000162828025010944/lee-20250212.htm	N/A	N/A	Lee Enterprises disclosed that a cybersecurity attack resulted in unauthorized access to its network, encryption of critical applications, and exfiltration of certain files, causing operational disruptions including delays in print distribution, billing, and vendor payments. The company stated the incident is reasonably likely to have a material impact on its financial condition or results of operations, with recovery efforts ongoing and the full scope of impact still under investigation.
National Presto Industries, Inc. (NPK)	3/6/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000080172/000143774925006475/npk20250306_8k.htm	N/A	N/A	N/A	N/A	National Presto disclosed that a cybersecurity incident caused a system outage that temporarily impacted operations, including shipping, manufacturing processes, and back-office functions, while restoration efforts are ongoing. The company stated the full scope remains under investigation and the incident could potentially have a material impact on its financial condition and results of operations.
Sensata Technologies Holding PLC (ST)	4/9/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001477294/000147729425000047/st-20250406.htm	N/A	N/A	N/A	N/A	Sensata disclosed that a ransomware incident encrypted certain devices on its network and resulted in temporary disruptions to operations, including shipping, manufacturing, and support functions, with some files also exfiltrated. The company stated it does not expect a material impact for the current quarter, but the full scope remains under investigation and could result in a future determination that the incident is material to its financial condition or results of operations.
Conduent Incorporated (CNDT)	4/14/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001677703/000167770325000067/cndt-20250409.htm#fact-identifier-26	N/A	N/A	N/A	N/A	Conduent disclosed that a threat actor gained unauthorized access to a limited portion of its environment, resulting in an operational disruption and the exfiltration of files containing personal information associated with a limited number of client end-users. The company stated the disruption did not materially impact operations, but it has incurred material non-recurring expenses related to notification requirements, with the full impact of the exfiltrated data still under analysis.
Nucor Corporation (NUE)	5/14/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000073309/000119312525119311/d795264d8k.htm	6/20/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000073309/000119312525143135/d92658d8ka.htm	N/A	N/A	Nucor disclosed that an unauthorized third party accessed certain IT systems, prompting the company to take affected systems offline and temporarily halt certain production operations at various locations. The company stated it is investigating and restarting operations, and has not yet determined the timing or materiality of the incident.

Form 8-K, Item 1.05 - Historical Filings

Issuer	Filing Date	Link to EDGAR Filing	Date of Amendment	Link to EDGAR Filing (Amendments)	Date of Comment Letter	Link to EDGAR Filing (Comment Letters)	Summary
Coinbase Global, Inc. (COIN)	5/15/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001679788/000167978825000094/coin-20250514.htm	N/A	N/A	N/A	N/A	Coinbase disclosed that threat actors obtained customer and internal data through insider-enabled unauthorized access by contractors or employees, including personal and account-related information, and issued an extortion demand. The company stated the incident did not involve access to passwords, private keys, or customer funds, and preliminarily estimated remediation and reimbursement costs of approximately $180 million to $400 million, with the full financial impact still under evaluation.
United Natural Foods, Inc. (UNFI)	6/26/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001020859/000102085925000036/unfi-20250621.htm	N/A	N/A	N/A	N/A	United Natural Foods disclosed that unauthorized activity on certain IT systems led the company to take systems offline, temporarily impacting its ability to fulfill and distribute customer orders before core systems were restored and operations normalized. The company stated the incident is reasonably likely to have a material impact on net income and adjusted EBITDA for the fourth quarter of fiscal 2025 due to reduced sales and increased costs, but does not expect a material impact on its overall financial condition.
Data I/O Corporation (DAIO)	8/21/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/351998/000165495425009925/daio_8k.htm	9/10/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000351998/000165495425010613/daio_8ka.htm	N/A	N/A	Data I/O disclosed that a ransomware incident affected certain internal IT systems, leading the company to take systems offline and resulting in temporary disruptions to operations including communications, shipping, manufacturing, and support functions. The company stated the incident does not appear to have had a material impact on operations to date, but expects related costs and recovery efforts to be reasonably likely to have a material impact on its financial condition and results of operations.
Wytec International, Inc. (WYTC)	8/29/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001560143/000168316825006583/wytec_8k.htm	2/3/2026	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001560143/000168316826000732/wytec_8ka1.htm	N/A	N/A	Wytec disclosed that a threat actor repeatedly defaced its website, prompting the company to take the site offline and restore it from backups while implementing additional security measures. The incident resulted in website downtime, cancellation of a scheduled seminar, and financial losses that the company expects to be significant but has not yet quantified.
F5, Inc. (FFIV)	10/15/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001048695/000104869525000149/ffiv-20251015.htm	N/A	N/A	N/A	N/A	F5 disclosed that a nation-state threat actor gained unauthorized, persistent access to certain systems, including its product development environment and knowledge management platform, and exfiltrated files containing portions of source code and information on vulnerabilities. The company stated it has contained the incident, found no evidence of impact to core systems such as CRM or financial platforms, and that the incident has not had a material impact on operations, with financial impact still under evaluation.
Jewett-Cameron Trading Company LTD. (JCTC)	10/21/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000885307/000107997325001631/jctc_8k.htm	N/A	N/A	N/A	N/A	Jewett-Cameron disclosed that a threat actor gained unauthorized access to portions of its IT environment, deployed encryption and monitoring software, and exfiltrated certain company information, including images of video meetings and computer screens, while causing disruptions and taking systems offline. The company stated the incident may materially impact operations due to downtime and could affect financial results, while the extent of any sensitive data compromise remains under investigation.
Bayfirst Financial Corp. (BAFN)	10/30/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001649739/000164973925000246/bafn-20251028.htm	N/A	N/A	N/A	N/A	BayFirst disclosed that a cybersecurity incident at a third-party marketing services provider resulted in unauthorized access to certain customer personal information, including names, dates of birth, and Social Security or tax identification numbers. The company stated the incident was limited to the third-party provider's environment, there is no evidence of misuse of the data, and it cannot yet quantify any material impact on its financial condition or operations.
Coupang, Inc. (CPNG)	12/16/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001834584/000183458425000196/cpng-20251215.htm#fact-identifier-25	12/29/2025	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001834584/000183458425000202/cpng-20251215.htm	N/A	N/A	Coupang disclosed that unauthorized access to customer accounts was linked to a former employee who obtained personal information, including names, phone numbers, addresses, email addresses, and certain order histories for up to 33 million accounts. The company stated no banking, payment, or login credential information was compromised, operations were not materially disrupted, and potential financial impacts, including regulatory penalties, cannot yet be estimated.

Form 8-K, Item 1.05 - Historical Filings

Issuer	Filing Date	Link to EDGAR Filing	Date of Amendment	Link to EDGAR Filing (Amendments)	Date of Comment Letter	Link to EDGAR Filing (Comment Letters)	Summary
UFP Technologies, Inc. (UFPT)	2/24/2026	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000914156/000162828026011152/ufpt-20260219.htm	N/A	N/A	N/A	N/A	UFP Technologies disclosed that an unauthorized third party accessed portions of its IT systems, exfiltrated certain files, and disrupted functions including billing and label making, while operations continued in all material respects. The company stated its systems have been largely restored, it is investigating the scope of any sensitive data accessed, and does not believe the incident has had or is reasonably likely to materially impact its financial condition or results of operations.
Trio-Tech International (TRT)	3/20/2026	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000732026/000143774926009193/trt20260320_8k.htm	N/A	N/A	N/A	N/A	Trio-Tech disclosed that a ransomware incident at a Singapore subsidiary resulted in the encryption of certain files and later escalated to unauthorized disclosure of company data, prompting containment measures and an investigation. The company stated the incident has not caused material operational disruption and is not expected to materially impact near-term financial results, but the full scope remains under investigation and could result in a future determination of material impact.
CareCloud, Inc. (CCLD)	3/27/2026	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001582982/000149315226013239/form8-k.htm	N/A	N/A	N/A	N/A	CareCloud disclosed that an unauthorized third party caused a temporary network disruption in its CareCloud Health division that impacted functionality and data access to one electronic health record environment for approximately 8 hours before full restoration. The company stated the incident was contained to that environment, is assessing whether patient data was accessed, and while it determined the incident to be material, it has not had a material impact on operations and is not reasonably likely to materially impact its financial condition or results of operations.
Bitcoin Depot Inc. (BTM)	4/8/2026	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001901799/000119312526147772/btm-20260406.htm	N/A	N/A	N/A	N/A	Bitcoin Depot disclosed that an unauthorized party gained access to certain IT systems and obtained credentials associated with its digital asset settlement accounts, resulting in the unauthorized transfer of approximately 50.903 Bitcoin valued at about $3.665 million. The company stated the incident was contained to its corporate environment with no evidence of customer data access, and while it determined the incident to be material, it does not believe it is reasonably likely to materially impact its financial condition or results of operations.
Stryker Corporation (SYK)	4/9/2026	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000310764/000119312526149607/d112875d8ka.htm	N/A	N/A	N/A	N/A	Stryker disclosed that a cybersecurity incident caused disruptions to its business operations, and subsequently determined that the incident had a material impact on operations and its financial results for the first quarter of 2026. The company stated that operations have been restored and it does not believe the incident is reasonably likely to have a material impact on its full-year 2026 financial guidance.
West Pharmaceutical Services, Inc. (WST)	5/11/2026	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000105770/000010577026000068/wst-20260507.htm	5/20/2026	https://www.sec.gov/ix?doc=/Archives/edgar/data/0000105770/000010577026000077/wst-20260507.htm	N/A	N/A	West Pharmaceutical Services experienced a cybersecurity attack involving data exfiltration and system encryption, prompting the company to take systems offline globally, engage external experts, and notify law enforcement while its investigation into scope and affected data remains ongoing. The incident and response efforts caused temporary global operational disruptions, though core systems and key manufacturing processes have since been restored and operations have resumed globally with no ongoing unauthorized access observed, and the company now believes the incident has not had and is not reasonably likely to have a material impact on its 2026 financial guidance.
CB Financial Services, Inc. (CBFV)	5/11/2026	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001605301/000160530126000021/cbfv-20260507.htm	N/A	N/A	N/A	N/A	CB Financial Services identified a material incident involving the use of unauthorized AI software that resulted in the exposure of sensitive non-public customer information, including names, Social Security numbers, and dates of birth, but did not disrupt operations or core systems. The company is investigating with external advisors, notifying affected parties and regulators, and implementing remediation measures, and does not expect the incident to have a material impact on its financial condition or results of operations.