



Acervus

CYBER RISK INTELLIGENCE

SAMPLE REPORT – FICTIONAL ORGANIZATIONS. ALL NAMES, DOMAINS, ADDRESSES, AND FINDINGS ARE INVENTED FOR ILLUSTRATION.

PORTFOLIO EXPOSURE MONITORING · MONTHLY REPORT

Sample Capital Partners September 2026

PREPARED FOR	Operating Partners, Sample Capital Partners (fictional)
PORTFOLIO COMPANIES	5 monitored
REPORTING PERIOD	September 1–30, 2026
REPORT DATE	October 2, 2026
REPORT ID	ACV-PEM-SAMPLE-2026-09
METHOD	Continuous passive, outside-in observation. Real-time alerts were sent during the month; this report summarizes them.

Public sample. Fictional organizations and findings; not a real client assessment.
Acervus, LLC | 153 E Flagler Street #223, Miami, FL 33131 | sales@acervusllc.com



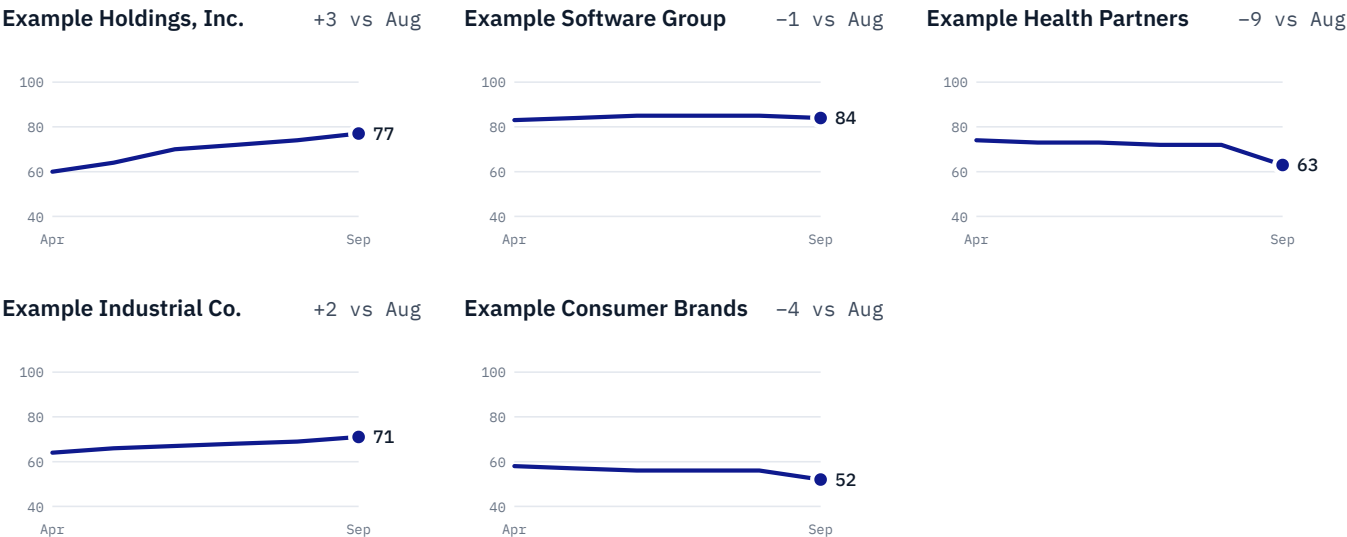
Executive summary

The portfolio's average exposure score fell from 71 to 69 in September. Two companies need attention: **Example Consumer Brands** exposed customer order files through a publicly listable cloud storage location, and **Example Health Partners** had a finance executive's credentials captured by infostealer malware. Both were alerted within hours and contained. **Example Holdings** continued to improve and has now closed every pre-acquisition finding that it controls. Health Partners and Consumer Brands also carry an elevated ransomware likelihood, with about **\$115,900** of combined revenue at risk for every hour of outage (see Potential financial impact).

PORTFOLIO AVERAGE	ALERTS SENT	RESOLVED THIS MONTH	OPEN CRITICAL/HIGH
69-2 vs Aug	5	4	3

COMPANY	SCORE	RATING	CHANGE	OPEN CRITICAL	OPEN HIGH	OPEN MEDIUM
Example Holdings, Inc.	77	Moderate	+3	0	0	0
Example Software Group	84	Low	-1	0	0	1
Example Health Partners	63	Elevated	-9	0	1	1
Example Industrial Co.	71	Moderate	+2	0	0	2
Example Consumer Brands	52	Elevated	-4	1	1	2

Exposure score, April–September 2026



All panels share the same scale (40–100). Score bands: Low 80–100, Moderate 65–79, Elevated 45–64, Severe 0–44.



Potential financial impact

Two portfolio companies, **Example Health Partners** and **Example Consumer Brands**, currently show conditions that make a successful ransomware attack more likely. Together they carry about **\$115,900 of revenue at risk for every hour** their core systems would be down. Example Industrial Co. has the largest exposure per hour because of its size, but its likelihood indicator has improved since Remote Desktop was removed from the internet.

COMPANY	ANNUAL REVENUE (ILLUSTRATIVE)	LIKELIHOOD INDICATOR	MAIN DRIVER THIS MONTH	REVENUE AT RISK PER HOUR	10-DAY OUTAGE
Example Health Partners	\$800M	■ ELEVATED	Finance director's credentials captured by infostealer malware; infected device still under investigation	\$63,900	\$15.3M
Example Consumer Brands	\$650M	■ ELEVATED	Lowest score in the portfolio (52); open critical finding; cloud storage was publicly exposed	\$51,900	\$12.5M
Example Industrial Co.	\$2.1B	■ MODERATE	Remote Desktop removed from the internet; manufacturing makes outages costly	\$167,800	\$40.3M
Example Software Group	\$450M	■ MODERATE	Database administration port newly reachable from the internet; fix scheduled	\$36,000	\$8.6M
Example Holdings, Inc.	\$1.2B	■ LOW	All pre-acquisition entry routes closed (credentials, VPN, Remote Desktop)	\$95,900	\$23.0M

HOW THE FIGURES ARE CALCULATED

Revenue at risk per hour = annual revenue ÷ 8,760 operating hours × 70%, the assumed share of revenue that depends on systems ransomware typically encrypts (order processing, ERP, production scheduling). Example Holdings: \$1,200,000,000 ÷ 8,760 = \$136,986 per hour × 70% = **\$95,890 per hour**. A 10-day outage is 240 hours; the average interruption reported for US ransomware victims was 24 days (Coveware, Q2 2022).

The likelihood indicator reflects externally observable conditions only: stolen credentials in circulation, internet-facing systems with known exploited vulnerabilities, exposed remote access, and extortion-site activity. It is not a prediction that an attack will or will not occur, and it cannot see internal controls such as multi-factor authentication, endpoint detection, segmentation, and tested backups. Revenue at risk is not lost profit, and the figures exclude response, recovery, legal, regulatory, and insurance costs and any ransom. Acervus replaces the illustrative revenue figures and the 70% assumption with figures confirmed by each company.

REFERENCE POINTS FROM PUBLIC INCIDENTS, INCLUDING INDIRECT ATTACKS THROUGH SUPPLIERS

- **MGM Resorts (2023):** a criminal cyberattack and system shutdown; about \$100 million loss reported to the SEC.
- **Delta Air Lines (2024):** not a cyberattack but a faulty vendor software update; more than 5,000 flights canceled and up to \$500 million in cost over five days, according to its CEO.



- **Quanta Computer (2021):** a ransomware group stole Apple product plans from the supplier and demanded \$50 million.
- **A.P. Moller-Maersk (2017):** indirect attack; NotPetya malware spread through a Ukrainian accounting software update and disabled Maersk's systems worldwide; cost estimated at \$200–300 million.
- **Target (2013):** indirect attack; intruders used an HVAC contractor's stolen credentials and took data from about 40 million payment cards; \$292 million in reported costs (\$202 million after insurance).

Sources: MGM Resorts Form 8-K, October 2023, as reported by NBC News; NPR, July 31, 2024; CNBC, April 21, 2021; Computer Weekly, August 2017 (Maersk Q2 2017 interim report); KrebsOnSecurity, February 2014; Target annual report, 2016, as reported by The SSL Store; Coveware quarterly data via Statista.



Alerts this month

DATE	COMPANY	ALERT	SEVERITY	STATUS
Sep 4	Example Health Partners	Three corporate accounts, including the finance director's, captured in infostealer malware logs	■ HIGH	Credentials reset Sep 5; infected device under investigation by the company
Sep 11	Example Consumer Brands	Publicly listable cloud storage location; file names indicate customer order exports. Acervus did not open or download any file.	● CRITICAL	Public access removed Sep 12; company counsel assessing notification obligations
Sep 17	Example Holdings, Inc.	TLS certificate on the customer portal due to expire in 14 days	■ LOW	■ RESOLVED Renewed Sep 20
Sep 22	Example Industrial Co.	New look-alike domain registered, no mail records yet	■ INFORMATIONAL	Watching for mail or web activity
Sep 26	Example Software Group	Database administration port newly reachable from the internet	■ MEDIUM	Company notified; fix scheduled

Also resolved this month

- **Example Holdings:** DMARC policy moved from none to reject, closing the last open pre-acquisition email finding.
- **Example Industrial Co.:** Remote Desktop removed from direct internet exposure.
- **Example Health Partners:** compromised credentials reset within one day of the alert.

Priorities for October

1. **Example Consumer Brands:** confirm counsel's notification decision, and review all cloud storage for public access settings.
2. **Example Health Partners:** obtain the result of the device investigation, and confirm multi-factor authentication covers all finance systems.
3. **Example Software Group:** confirm the database port is closed by the scheduled date.



Since acquisition: Example Holdings, Inc.

Example Holdings scored 58 (Elevated) in the March 2026 Pre-Diligence Exposure Assessment. Six months after closing it scores 77 (Moderate). Every finding the company controls has been resolved.

ID	PRE-DILIGENCE FINDING	STATUS	CLOSED
F-01	Credentials in infostealer logs	RESOLVED	Apr
F-02	VPN appliance with known exploited vulnerability; compromise assessment found no evidence of intrusion	RESOLVED	Apr
F-03	Extortion-site listing naming a subsidiary; addressed in confirmatory diligence	CLOSED IN DILIGENCE	Mar
F-04	Weak email authentication	RESOLVED	Sep
F-05	Remote Desktop exposed to the internet	RESOLVED	May
F-06	Dangling subdomain records	RESOLVED	Jun
F-07	Historical breach exposure	MONITORED	—
F-08	Look-alike domain with mail records; taken down after a registrar complaint	RESOLVED	Jul

About this report

- Monitoring is passive and outside-in, using licensed breach and infostealer intelligence, internet-wide scan data, DNS and certificate records, and extortion-site monitoring. No company systems are tested or accessed.
- Scores are comparable month to month and across companies because the same indicators and weights apply to each.
- The absence of an alert is not evidence that no risk or compromise exists. This report is not an audit opinion or legal advice.

