



Acervus

CYBER RISK INTELLIGENCE

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

PRE-DILIGENCE EXPOSURE ASSESSMENT

Example Holdings, Inc.

PREPARED FOR	Sample Capital Partners (fictional)
TARGET	Example Holdings, Inc. and subsidiaries; primary domain exampleholdings.example
OBSERVATION PERIOD	March 9–13, 2026
REPORT DATE	March 16, 2026
REPORT ID	ACV-PDA-SAMPLE-001
METHOD	Passive, outside-in observation. No systems belonging to the target were tested, accessed, or contacted beyond ordinary public web and DNS requests.

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

Example Holdings presents an **elevated** external cyber risk profile. Three findings warrant attention before significant diligence resources are committed: active credential exposure affecting remote access accounts, an internet-facing VPN appliance running firmware with a vulnerability known to be exploited in the wild, and a 2025 listing naming a subsidiary on a ransomware extortion site with no matching public disclosure. Based on these findings, the likelihood of a successful ransomware attack is **elevated**, and each hour of outage would put an estimated **\$95,900** of revenue at risk (see Potential financial impact below).



What this means for the transaction

- **Possible undisclosed incident.** The extortion-site listing (F-03), combined with recent credential theft (F-01), raises a reasonable question about whether a prior compromise occurred and how it was handled.
- **Near-term remediation cost.** F-01 and F-02 require prompt action by the target regardless of deal outcome; their status at signing is a reasonable diligence request.
- **Payment-fraud exposure.** Weak email authentication (F-04) and an active look-alike domain (F-08) increase the risk of impersonation during the transaction itself, including fraudulent payment instructions.

Questions for confirmatory diligence

1. Has the company experienced a cybersecurity incident, extortion demand, or data exposure since January 2024? If so, provide the incident report, notifications made, and insurer correspondence.
2. Provide evidence that the accounts referenced in F-01 have had credentials reset and sessions revoked, and that multi-factor authentication is enforced on remote access.
3. Confirm the current firmware version and patch date of the VPN appliance referenced in F-02, and whether a compromise assessment was performed.
4. Provide the company's cyber insurance policy, claims history, and most recent application.

Acervus recommends wire-transfer verification by telephone, using independently sourced numbers, for all payments related to this transaction.



Potential financial impact

Acervus estimates what a successful ransomware attack could cost Example Holdings in revenue while its systems are down, and how the findings in this report affect the likelihood of such an attack.

RANSOMWARE LIKELIHOOD INDICATOR

ELEVATED

Three common ransomware entry routes observed at once

REVENUE AT RISK PER HOUR OF OUTAGE

\$95,900

About \$2.3 million per day, using the assumptions below

WHY THE LIKELIHOOD IS ELEVATED

CONDITION ASSOCIATED WITH RANSOMWARE INTRUSIONS	OBSERVED	FINDING
Stolen credentials for remote access in circulation	● YES	F-01
Internet-facing system with a known exploited vulnerability	■ YES	F-02
Remote Desktop exposed directly to the internet	■ YES	F-05
Prior listing on a ransomware extortion site	■ YES	F-03
Email spoofing protections enforced	■ NO	F-04

Stolen credentials, exploitation of internet-facing systems, and exposed remote access are among the most common ways ransomware operators gain initial access. With all three present at the same time, and a prior extortion-site listing, Acervus rates the likelihood indicator **Elevated**. Closing F-01, F-02, and F-05 would be expected to lower it to Moderate or Low.

The indicator compares the target with organizations that do not show these conditions. It is not a prediction that an attack will or will not occur. It cannot reflect internal controls that are not visible from outside, such as multi-factor authentication coverage, endpoint detection, network segmentation, and tested backups, all of which strongly affect both likelihood and recovery time.

DOWNTIME COST EXAMPLE

		OUTAGE LENGTH	REVENUE AT RISK
Annual revenue (illustrative)	\$1,200,000,000		
Operating hours per year (24 × 365)	8,760	3 days: fast restoration from clean, tested backups	\$6.9M
Revenue per hour	\$136,986	10 days	\$23.0M
Share of revenue that depends on systems ransomware typically encrypts (assumption)	70%	24 days: average interruption reported for US ransomware victims (Coveware, Q2 2022)	\$55.2M
Revenue at risk per hour	\$95,890		



Revenue at risk is not the same as lost profit; some sales are deferred rather than lost. The estimate excludes incident response and forensics, rebuilding systems, legal counsel and breach notification, regulatory penalties, lost customers, higher insurance costs, and any ransom. Together these often equal or exceed the lost revenue. Acervus replaces the illustrative revenue figure and the 70% assumption with figures confirmed by the client.

For the transaction: this exposure can be discussed with counsel when setting remediation conditions before closing, escrow or specific indemnity, and representations and warranties coverage.

REFERENCE POINTS FROM PUBLIC INCIDENTS, INCLUDING INDIRECT ATTACKS THROUGH SUPPLIERS

- **MGM Resorts (2023).** A criminal cyberattack led the company to shut down systems; MGM reported a loss of about \$100 million in a filing with the SEC.
- **Delta Air Lines (2024).** Not a cyberattack: a faulty software update from a security vendor took systems offline. Delta canceled more than 5,000 flights, and its CEO put the cost at up to \$500 million over five days. Downtime alone becomes expensive quickly, before any ransom or data theft.
- **Quanta Computer (2021).** A ransomware group stole product plans belonging to Apple, a Quanta customer, and demanded \$50 million. A supplier's breach can expose its customers' most sensitive information.
- **A.P. Moller-Maersk (2017).** Indirect attack: the NotPetya malware, aimed mainly at organizations in Ukraine, spread through the automatic update of a Ukrainian accounting software package and disabled Maersk's systems worldwide. Maersk estimated the cost at \$200 million to \$300 million.
- **Target (2013).** Indirect attack: intruders entered Target's network with credentials stolen from an HVAC contractor and took data from about 40 million payment cards. Target reported \$292 million in breach-related costs (\$202 million after insurance) through 2016.

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.



Findings summary

ID	FINDING	SEVERITY	CATEGORY	OBSERVED
F-01	Corporate credentials, including two with remote access privileges, present in recent infostealer malware logs	CRITICAL	Credentials	Mar 10
F-02	Internet-facing VPN appliance running firmware with a known exploited vulnerability	HIGH	Infrastructure	Mar 9
F-03	Subsidiary named on a ransomware group's extortion site (March 2025); no public disclosure located	HIGH	Incident history	Mar 11
F-04	Primary domain DMARC policy set to "none"; two secondary domains have no SPF record	MEDIUM	Email	Mar 9
F-05	Remote Desktop service exposed directly to the internet	MEDIUM	Infrastructure	Mar 9
F-06	Three subdomains point to decommissioned cloud resources (takeover risk)	MEDIUM	Domains	Mar 12
F-07	212 employee addresses appear in four historical third-party breaches (2019–2023)	LOW	Credentials	Mar 10
F-08	Look-alike domain registered in February 2026 with active mail records	INFORMATIONAL	Domains	Mar 12

Severity reflects potential business impact and likelihood of exploitation as observed from outside the organization. Dates are 2026 unless stated.



Detailed findings

F-01 · Credentials in infostealer logs

● CRITICAL

OBSERVATION	Seven corporate accounts on exampleholdings.example appear in infostealer malware logs collected between December 2025 and March 2026. Two of the associated logins were captured for the company's remote access portal.
EVIDENCE	j.****@exampleholdings.example · r.*****@exampleholdings.example · 5 further accounts (full list provided to the recipient separately). Passwords are never reproduced in Acervus reports.
WHY IT MATTERS	Infostealer logs typically include session cookies and saved passwords taken from an infected device. Access of this kind is commonly sold to ransomware operators.
RECOMMENDED ACTION	Target: reset affected credentials, revoke active sessions, enforce multi-factor authentication on remote access, and examine the infected devices. Buyer: request evidence of completion.

F-02 · VPN appliance with a known exploited vulnerability

■ HIGH

OBSERVATION	The VPN appliance at 203.0.113.24 reports a firmware version affected by a remote code execution vulnerability listed in CISA's Known Exploited Vulnerabilities catalog.
WHY IT MATTERS	Unpatched edge devices are among the most frequent initial access points in ransomware intrusions. Because exploitation is confirmed in the wild, compromise may have occurred before any patch is applied.
RECOMMENDED ACTION	Target: patch immediately and perform a compromise assessment of the appliance. Buyer: request patch records and assessment results.

F-03 · Extortion-site listing naming a subsidiary

■ HIGH

OBSERVATION	A March 2025 listing on a ransomware group's data-leak site names Example Logistics LLC (fictional), a subsidiary of the target, and claims possession of internal documents. No regulatory filing, press report, or breach notification corresponding to this listing was located.
WHY IT MATTERS	Listings are claims by criminal groups and are not proof of compromise. However, an undisclosed incident may carry notification obligations, regulatory exposure, and residual adversary access.
RECOMMENDED ACTION	Buyer: raise directly in confirmatory diligence (question 1) and in the representations and warranties discussion with counsel.

F-04 · Weak email authentication

■ MEDIUM

OBSERVATION	The primary domain publishes a DMARC policy of p=none, which reports on but does not block spoofed email. Two secondary domains publish no SPF record.
WHY IT MATTERS	Attackers can send email that appears to come from the company, a common route to fraudulent payment instructions.
RECOMMENDED ACTION	Target: move DMARC to quarantine and then reject after reviewing reports; publish SPF on all domains, including those that send no email.



F-05 · Remote Desktop exposed to the internet

■ MEDIUM

OBSERVATION	Remote Desktop Protocol is reachable at 198.51.100.17:3389.
RECOMMENDED ACTION	Target: remove direct exposure and place remote administration behind the VPN with multi-factor authentication.

F-06 · Dangling subdomain records

■ MEDIUM

OBSERVATION	promo., legacy-portal., and files-old. exampleholdings.example point to cloud resources that no longer exist.
RECOMMENDED ACTION	Target: delete the records or reclaim the resources, so a third party cannot host content under the company's domain.

F-07 · Historical breach exposure

■ LOW

OBSERVATION	212 company email addresses appear in four third-party breaches between 2019 and 2023. This is typical for an organization of this size and is noted for completeness.
-------------	--

F-08 · Look-alike domain with mail records

■ INFORMATIONAL

OBSERVATION	exampleholding.example (missing "s") was registered in February 2026 by an unrelated party and has active mail records, a common precursor to impersonation.
RECOMMENDED ACTION	Target: monitor and, if abused, pursue takedown. Buyer: apply telephone verification to all deal payments.



Scope, method, and limitations

Scope

The primary domain, 4 secondary domains, 37 subdomains, and 11 internet-facing IP addresses attributed to the target and its subsidiaries through public registration, DNS, and certificate records.

Sources

- Licensed breach and infostealer intelligence
- Internet-wide scan data
- DNS, WHOIS, and certificate transparency records
- Monitoring of public extortion and leak sites
- Public filings, press, and regulatory records

Scoring

The exposure score starts at 100 and deducts weighted points for each finding by severity and recency, capped per category so that one issue type cannot dominate.

RATING	SCORE
Low	80–100
Moderate	65–79
Elevated	45–64
Severe	0–44

Limitations

- This assessment is passive and outside-in. It reflects what was observable during the observation period and cannot see internal systems, controls, or activity.
- The absence of a finding is not evidence that no risk or compromise exists.
- Extortion-site listings and breach data are third-party claims; Acervus reports them with their source type and date and does not verify them against the target's records.
- This report is not an audit opinion, a certification, or legal advice.

Acervus can convert this assessment into Portfolio Exposure Monitoring after closing, measuring the same indicators monthly with alerts on material change.

