

BÁO CÁO PHÂN TÍCH NGÀNH

THÁCH THỨC MỚI

Quản trị An toàn tài sản số ngành logistics

Công ty Cổ phần An ninh mạng 405CYSE

www.405cyse.com

Tổng quan

Logistics là mắt xích nối mọi ngành kinh tế và cũng là nơi dữ liệu cá nhân đi qua nhiều tay nhất. Mỗi vận đơn mang theo tên, số điện thoại, địa chỉ và giá trị hàng của người nhận. Năm 2025 thị trường bưu chính Việt Nam xử lý khoảng 4,1 tỷ bưu gửi, hơn 90% là hàng hóa.

Thương mại điện tử và chuyển đổi số buộc doanh nghiệp logistics kết nối liên tục với sàn, chủ hàng, nhà xe và cơ quan quản lý. Với logistics B2B, mỗi lô hàng còn kèm chứng từ, giá cước và dòng tiền của chủ hàng. Mỗi kết nối giúp hàng đi nhanh hơn nhưng cũng mở thêm 1 lối vào cho tin tặc và cho người lạm dụng quyền truy cập. Vụ Vietnam Post bị mã độc tống tiền, dữ liệu vận đơn của GHN bị rao bán làn sóng lừa đảo giả danh shipper và các email giả đổi tài khoản thanh toán nhắm vào doanh nghiệp xuất nhập khẩu cho thấy rủi ro đã hiện diện tại Việt Nam. **Báo cáo cho thấy phần lớn doanh nghiệp không thiếu công cụ mà thiếu quy trình và người chịu trách nhiệm cho dữ liệu đi qua tay mình.**

4,1 TỶ BƯU GỬI

Sản lượng bưu gửi năm 2025, hơn 90% là gói, kiện hàng hóa. Sản lượng tăng hơn 4 lần so với năm 2020.

Bộ Khoa học và Công nghệ, 2026

283 VỤ

Vụ tấn công mã độc tống tiền vào doanh nghiệp vận tải và logistics toàn cầu năm 2025, nhiều hơn tổng của 2 năm 2023 và 2024.

Cyble, 2026



52,30%

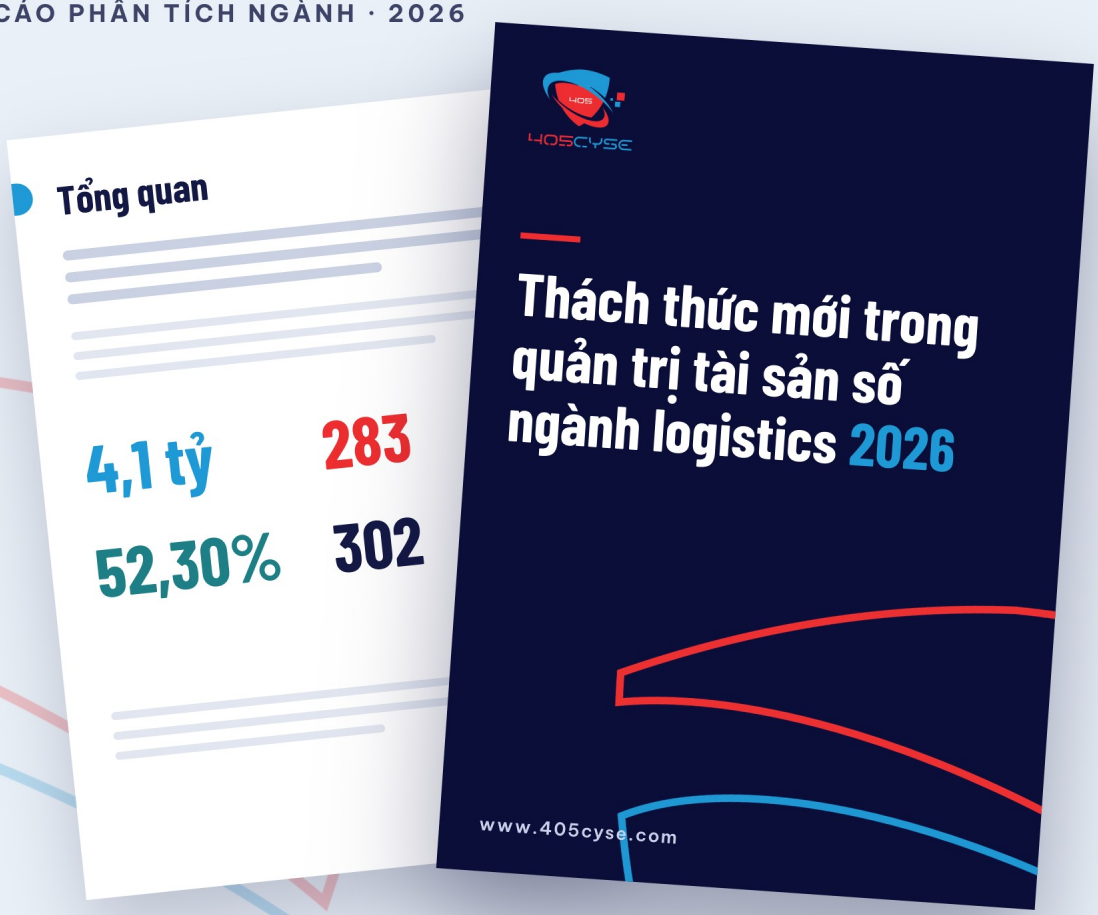
Tỷ lệ cơ quan và doanh nghiệp Việt Nam chịu thiệt hại do tấn công mạng năm 2025. Số liệu này áp dụng chung cho mọi ngành.

NCA, 2026

302 VỤ LỘ LỌT

Vụ lộ lọt dữ liệu liên quan đến Việt Nam được ghi nhận trên diễn đàn ngầm nửa đầu năm 2026, tăng 58,1% so với cùng kỳ.

Viettel Cyber Security, 2026



Nội dung

01	Dữ liệu là hàng hóa thứ hai trên mỗi chuyến xe	Trang 5
02	Rủi ro mới đối với dữ liệu trong chuỗi giao nhận	Trang 10
03	Chi phí hữu hình và chi phí chìm của sự cố	Trang 17
04	Những khoảng trống đòi hỏi thay đổi tư duy quản trị an toàn dữ liệu	Trang 21
05	Quản trị an toàn tài sản số phục vụ tăng trưởng	Trang 24
	Kết luận	Trang 27

Tiêu chí	Hệ thống văn phòng	Hệ thống hiện trường
Hệ thống tiêu biểu	ERP, kế toán, hóa đơn điện tử, hệ thống đối soát thu hộ (COD), CRM và tổng đài, thư điện tử, phần mềm nhân sự	OMS (quản lý đơn hàng), TMS (quản lý vận tải), WMS (quản lý kho), FMS (quản lý đội xe), YMS (quản lý bãi container), TOS (khai thác cảng), phần mềm khai báo hải quan, cổng API và EDI với sàn, chủ hàng, ứng dụng shipper và tài xế, máy quét PDA, dây chuyền chia chọn, thiết bị giám sát hành trình
Người dùng	Hàng chục đến vài trăm nhân viên văn phòng	Hàng nghìn shipper, tài xế, nhân viên kho, bưu cục, đại lý và cộng tác viên, nhiều người làm thời vụ
Thiết bị	Máy tính do doanh nghiệp quản lý	Điện thoại cá nhân, PDA và máy in nhãn dùng chung, Wi-Fi kho, camera CCTV, máy tính tại bưu cục và đại lý
Ưu tiên bảo vệ	Tính bí mật của dữ liệu	Tính sẵn sàng: hàng phải đi đúng giờ

THỜI GIAN NGỪNG CHẤP NHẬN ĐƯỢC

Văn phòng	Có thể tính bằng giờ
Hiện trường	Tính bằng phút vào giờ cao điểm

NGƯỜI XEM ĐƯỢC DỮ LIỆU NGƯỜI NHẬN

Văn phòng	Vài chục người
Hiện trường	Hàng nghìn người, thay đổi liên tục

Sự khác biệt này là gốc rễ của nhiều rủi ro. Dữ liệu cá nhân của người nhận nằm trong tay lực lượng hiện trường đông đảo, biến động và dùng thiết bị doanh nghiệp không kiểm soát. Trong khi đó, biện pháp bảo mật thường chỉ tập trung vào hệ thống văn phòng.

1.4. Bản đồ tài sản số theo hành trình đơn hàng

Dữ liệu logistics di chuyển cùng hàng hóa qua nhiều đơn vị và không dừng lại trong ranh giới của 1 doanh nghiệp. Báo cáo gọi chung dữ liệu, hệ thống văn phòng, hệ thống hiện trường, các kết nối với đối tác cùng quyền truy cập mà doanh nghiệp cần bảo vệ là **tài sản số**. Hình 1 cho thấy tài sản số có giá trị xuất hiện ở mọi chặng của 1 đơn hàng.

1.6. Logistics B2B: dữ liệu của chủ hàng và chứng từ thương mại

Bên cạnh chuyển phát thương mại điện tử, ngành logistics Việt Nam còn có mảng B2B rộng lớn gồm giao nhận vận tải quốc tế, kho vận hợp đồng (3PL), vận tải container, kho lạnh, kho ngoại quan, cảng cạn (ICD) và khai thuê hải quan. Năm 2025 tổng kim ngạch xuất nhập khẩu của Việt Nam vượt 930 tỷ USD (RMIT Việt Nam, 2026). Khách hàng của mảng B2B là doanh nghiệp, nên tài sản dữ liệu nhạy cảm nhất là chứng từ, dòng tiền và bí mật thương mại của chủ hàng.

Nhóm tài sản	Hệ thống và dữ liệu tiêu biểu	Hậu quả khi bị xâm phạm
Chứng từ vận tải và thương mại	Booking, vận đơn đường biển (B/L), vận đơn hàng không (AWB), lệnh giao hàng điện tử (eDO), hóa đơn thương mại, C/O	Hàng bị lấy sai người, chứng từ bị làm giả, tranh chấp với chủ hàng và hãng tàu
Khai báo hải quan	Phần mềm khai báo kết nối VNACCS/VCIS, chữ ký số của doanh nghiệp, trị giá khai báo	Khai báo sai hoặc bị khai thay, lộ trị giá và nguồn hàng của chủ hàng
Dữ liệu chủ hàng trong kho vận 3PL	Tồn kho, đơn hàng và kế hoạch phân phối trong WMS, cổng thông tin cho chủ hàng	Lộ bí mật thương mại; tồn kho sai làm đứt chuỗi cung ứng của chủ hàng
Giá cước và hợp đồng	Bảng giá, hợp đồng với hãng tàu, hãng bay, báo giá cho khách hàng	Đối thủ có lợi thế đàm phán; doanh nghiệp vi phạm cam kết bảo mật
Thanh toán quốc tế	Email với chủ hàng và đại lý nước ngoài, hóa đơn cước, phí địa phương, tài khoản nhận tiền	Tiền cước chuyển vào tài khoản của kẻ gian qua email giả mạo (BEC)
Cảng điện tử và thiết bị IoT	Tài khoản ePort, cảm biến nhiệt độ kho lạnh và container lạnh, cổng tự động	Container bị lấy trái phép; dữ liệu nhiệt độ bị sửa khiến thực phẩm, dược phẩm phải hủy

CẢNG ĐIỆN TỬ ĐÃ TRỞ THÀNH HẠ TẦNG CHUNG

Từ năm 2018 cảng Tân Cảng – Cát Lái áp dụng cảng điện tử ePort cho 100% phương án giao nhận container và triển khai lệnh giao hàng điện tử với hãng tàu (VnEconomy, 2026). Cảng, hãng tàu, công ty giao nhận và nhà xe cùng thao tác trên một nền tảng dữ liệu chung. Tài khoản ePort của doanh nghiệp giao nhận vì vậy có giá trị như chìa khóa nhận hàng.

YÊU CẦU TỪ CHỦ HÀNG

Chủ hàng đa quốc gia ngày càng yêu cầu nhà cung cấp logistics trả lời bảng câu hỏi an ninh thông tin, chứng minh ISO/IEC 27001 hoặc chấp nhận đánh giá trước khi ký hợp đồng. Với doanh nghiệp B2B, an toàn dữ liệu là điều kiện để giữ khách hàng.

02

Rủi ro mới đối với dữ liệu trong chuỗi giao nhận

Doanh nghiệp có thể gặp 3 kiểu tổn hại dữ liệu là lộ lọt, thay đổi trái phép và mất khả năng truy cập. Mỗi kiểu có cơ chế và hậu quả riêng.

2.1. Bức tranh tổng quan

Tin tặc và người lạm dụng quyền truy cập kết hợp nhiều hướng: đánh cắp dữ liệu để rao bán hoặc tống tiền, làm tê liệt hệ thống để gây áp lực và thay đổi dữ liệu đơn hàng để chiếm đoạt tiền, hàng. Các hướng này tương ứng với 3 thuộc tính bí mật, toàn vẹn và sẵn sàng của dữ liệu.

Lộ lọt
Mất tính bí mật

DỮ LIỆU CHỊU ẢNH HƯỞNG

Thông tin người nhận, giá trị thu hộ, chứng từ và giá cước của chủ hàng

HẬU QUẢ VỚI DOANH NGHIỆP

Khách hàng bị lừa đảo, mất uy tín với sàn và chủ hàng, chịu xử phạt

Thay đổi trái phép
Mất tính toàn vẹn

DỮ LIỆU CHỊU ẢNH HƯỞNG

Địa chỉ giao, trạng thái đơn, tài khoản nhận tiền, lệnh giao hàng, đặt chỗ

HẬU QUẢ VỚI DOANH NGHIỆP

Giao nhầm, mất hàng, thanh toán sai, khiếu nại hàng loạt

Mất truy cập
Mất tính sẵn sàng

DỮ LIỆU CHỊU ẢNH HƯỞNG

OMS, TMS, WMS, ứng dụng shipper, cổng kết nối với sàn và chủ hàng

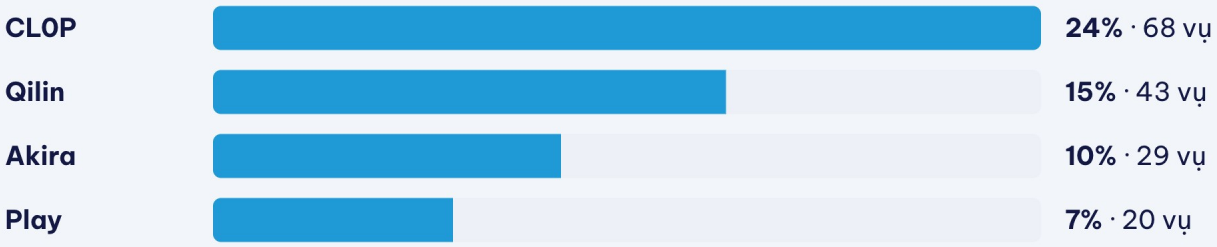
HẬU QUẢ VỚI DOANH NGHIỆP

Hàng ùn ứ, lỡ chuyến, chậm đối soát thu hộ, mất sản lượng

2.2. Phân loại các nhóm rủi ro

Báo cáo chia rủi ro đối với dữ liệu logistics thành 8 nhóm. Mỗi nhóm gắn với 1 đặc thù vận hành đã nêu tại mục 1.5 và 1.6.

04 nhóm mã độc gây ra 57% số vụ nhắm vào logistics



Hình 2. Tỷ trọng các nhóm mã độc tống tiền trong 283 vụ tấn công vào doanh nghiệp vận tải và logistics năm 2025. Nguồn: Cyble

2.2.5.

Rủi ro từ bên thứ ba và nền tảng kết nối

40% vụ lộ lọt 9 tháng 2025 tại Việt Nam qua bên thứ ba

ĐẶC THÙ LIÊN QUAN	Doanh nghiệp kết nối với sàn, phần mềm bán hàng, nền tảng CRM, đại lý, nhà xe và đơn vị CNTT thuê ngoài. Doanh nghiệp logistics cũng là bên thứ ba của chủ hàng.
HIỆN TRẠNG	Khoảng 40% vụ lộ lọt dữ liệu tại Việt Nam trong 9 tháng đầu năm 2025 xảy ra qua bên thứ ba (Viettel Cyber Security, 2025). Theo Verizon DBIR 2026, 48% vụ vi phạm dữ liệu có liên quan đến bên thứ ba.
CƠ CHẾ	API Key dùng chung, tài khoản tích hợp có quyền rộng và nền tảng đám mây bị chiếm quyền làm dữ liệu rời doanh nghiệp mà hệ thống nội bộ không ghi nhận.
DẪN CHỨNG	Tháng 10/2025 Vietnam Airlines xác nhận dữ liệu khoảng 7,3 triệu khách hàng bị lộ từ nền tảng chăm sóc khách hàng do đối tác công nghệ quốc tế vận hành. Cùng thời gian, dữ liệu mua sắm của nền tảng quản lý bán hàng Sapo cũng bị rao bán (Báo Đầu tư, 2025).

2.2.6.

Rủi ro gian lận đơn hàng và đánh cắp hàng hóa

34 tỷ USD thiệt hại mỗi năm do trộm cắp hàng hóa tại Hoa Kỳ

ĐẶC THÙ LIÊN QUAN	Đơn hàng, lệnh điều xe, sàn ghép chuyến và đối soát thu hộ được xử lý qua tài khoản trực tuyến.
HIỆN TRẠNG	Từ tháng 8/2025 Proofpoint ghi nhận gần 2 chục chiến dịch nhắm vào doanh nghiệp vận tải Bắc Mỹ. Tin tặc cài phần mềm điều khiển từ xa hợp lệ, chiếm tài khoản trên sàn ghép chuyến rồi nhận chở hàng thật để đánh cắp (Proofpoint, 2025).
CƠ CHẾ	Tại Việt Nam, đối tượng tạo đơn ảo nhờ shipper mua hộ hàng, giả danh đơn vị giao hàng để đòi chuyển khoản hoặc chiếm tài khoản để đổi địa chỉ giao và tài khoản nhận tiền thu hộ.
TÁC ĐỘNG	Doanh nghiệp mất tính toàn vẹn của dữ liệu và mất trực tiếp tiền, hàng. Shipper và người nhận là nạn nhân đầu tiên.

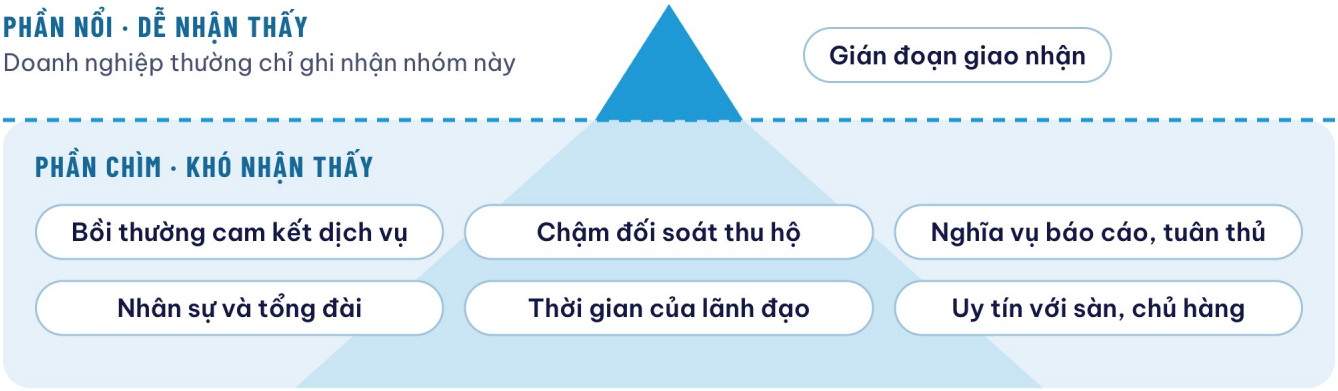
03

Chi phí hữu hình và chi phí chìm của sự cố

Tiền chuộc chỉ là phần nổi. Phần lớn thiệt hại nằm ở hàng ùn ứ, dòng tiền thu hộ, nghĩa vụ pháp lý và niềm tin của chủ hàng.

3.1. Các nhóm chi phí của mỗi sự cố

Thiệt hại của mỗi sự cố gồm gián đoạn giao nhận, bồi thường cam kết dịch vụ, chậm đối soát thu hộ, nghĩa vụ báo cáo và tuân thủ, chi phí nhân sự và uy tín với sàn, chủ hàng. Doanh nghiệp thường chỉ ghi nhận nhóm đầu tiên nên đánh giá thấp thiệt hại thực tế.



3.2. Đình trệ nghĩa vụ pháp lý và tài chính

Khi mất dữ liệu đơn hàng, cước và thu hộ thì doanh nghiệp có thể chậm lập hóa đơn điện tử, chậm khai thuế, chậm trả tiền thu hộ cho chủ shop và chậm khai báo hải quan với hàng xuất nhập khẩu. Đối soát lại hàng trăm nghìn đơn sau sự cố thường kéo dài hơn chính thời gian hệ thống ngừng.