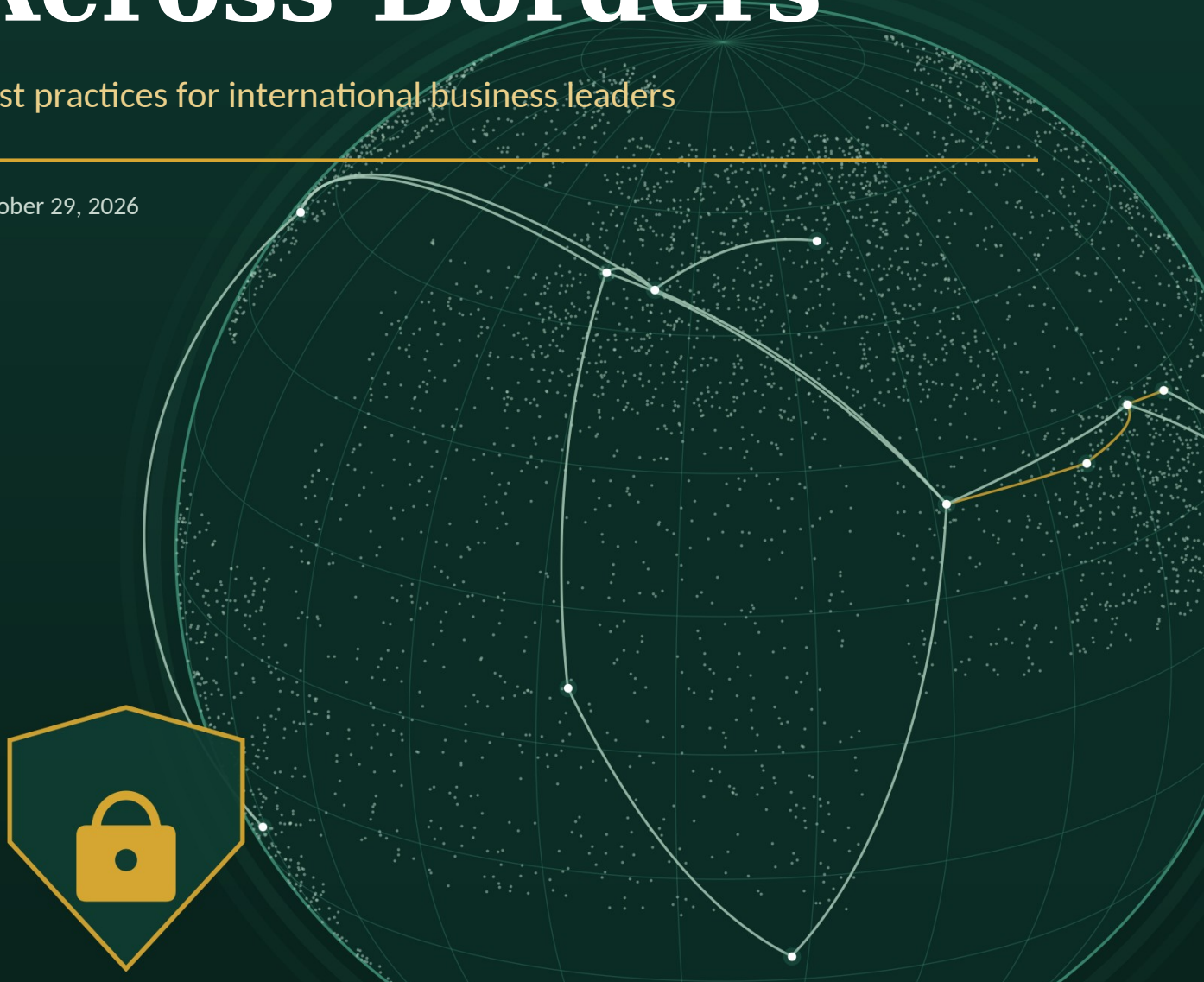
Tralphium $^{3}_{2}$He
STRATEGIC ADVISORY

WHITE PAPER

Cybersecurity Across Borders

Best practices for international business leaders

October 29, 2026



About this paper

AUTHOR	Donald Marzullo
PUBLISHER	Tralphium, LLC
DATE	October 29, 2026
AUDIENCE	Board members, executives, security leaders, legal and privacy teams, procurement, and business continuity managers

Executive summary

International businesses rely on digital services that connect employees, customers, suppliers, and facilities across national borders. These connections support growth but can also carry disruption from one location to another. A single incident may interrupt operations, expose personal information, affect partners, and trigger several distinct reporting obligations.

The recommended approach combines clear enterprise accountability and a common security baseline with local expertise and legal requirements. Leaders should identify essential business services, map their dependencies, protect high-impact access and data, plan with critical suppliers, and rehearse recovery across jurisdictions. The objective is to maintain essential services and make timely decisions when information is incomplete.

EIGHT PRACTICES AT A GLANCE

01 Establish accountability and decision rights
02 Identify critical services and dependencies
03 Maintain a jurisdiction and obligations register
04 Apply and verify a global security baseline
05 Manage suppliers by business impact
06 Govern international data flows
07 Prepare people and rehearse response
08 Measure outcomes and improve

The international risk landscape

A cyber event can begin locally and become global. In 2017, the NotPetya malware entered A.P. Moller–Maersk through software used for tax filing in Ukraine. It disrupted transport and logistics operations and forced the company to use manual workarounds. Maersk estimated losses of $250 million to $300 million, including lost revenue and restoration and extraordinary operating costs. The case illustrates how a local software dependency can affect a global business and its customers. [1, 2]

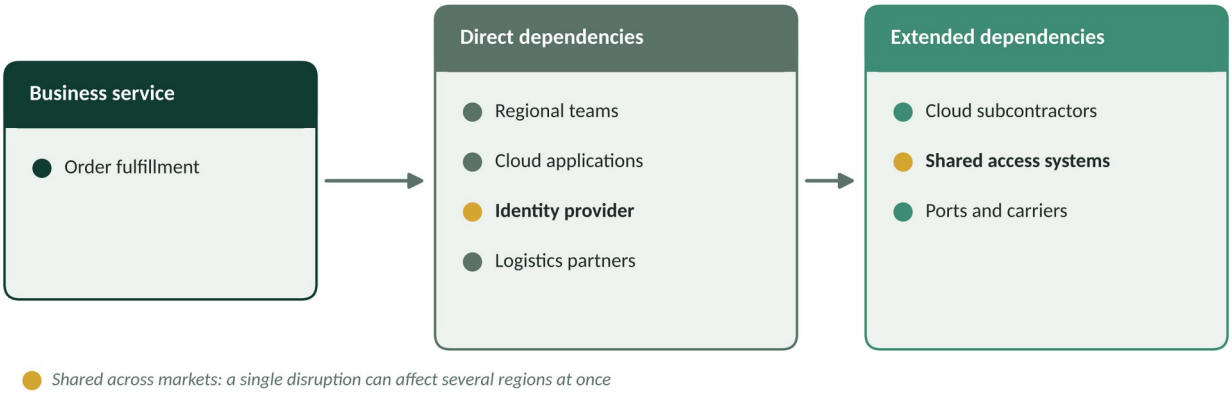
CASE IN POINT

$250–300 million

Maersk's estimated losses from NotPetya in 2017, after malware entered through tax-filing software used in a single country. [1, 2]

Cross-border exposure also includes geopolitical tensions, uneven security capabilities, shared service providers, and differences in laws and contractual duties. The UK National Cyber Security Centre has warned of disruptive activity by state and non-state actors and increased targeting of operational technology: systems that monitor or control physical processes such as production lines. [3]

FIGURE 1 **Map dependencies around the business service**



Illustrative. Replace the examples with the organization's actual dependencies and identify which are shared across markets. A shared identity provider, for example, may support several apparently separate regional applications; its disruption could therefore affect multiple markets at once.

A coordinated operating model

The board sets risk tolerance and oversees management. Executives assign accountability and fund resilience. Central security and support teams establish minimum controls and coordinate monitoring and response. Regional leaders implement those controls, identify local requirements, and report exceptions. Business and supplier owners maintain the services and relationships the organization relies on.

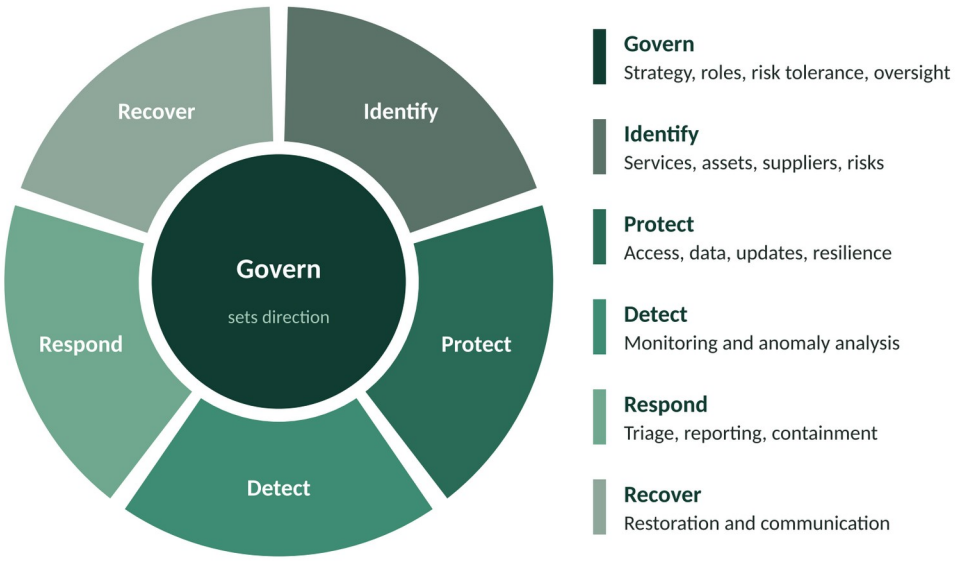
© 2026 Tralphium, LLC · Author: Donald Marzullo

TABLE 1 Responsibilities by level

LEVEL	PRIMARY RESPONSIBILITY	KEY DECISION
Board and executives	Set priorities, risk tolerance and oversight	Which disruptions are unacceptable?
Central security and support	Set baseline controls and coordinate response	What must every location implement?
Regional and local leaders	Apply controls and identify local obligations	What local requirements or constraints apply?
Service and supplier owners	Maintain operations and dependencies	How will the service continue or recover?

The National Institute of Standards and Technology (NIST), a United States government standards agency, provides a useful organizing structure in its Cybersecurity Framework 2.0: govern, identify, protect, detect, respond, and recover. The framework describes outcomes and is adaptable to organizations of different sizes and sectors. [4]

FIGURE 2 NIST Cybersecurity Framework 2.0 functions



Eight practices for international resilience

01 Establish accountability and decision rights

Assign an executive owner for cyber risk and a business owner for every critical service. Define who can isolate a system, accept an exception, notify a regulator, approve public communications, and authorize

restoration. Include security and resilience in acquisition, outsourcing, and market-entry decisions. Maintain an enterprise risk register that records owners, actions, deadlines, and decisions on residual risk—the risk that remains after controls are applied.

02 Identify critical services and dependencies

Select services whose failure would cause material harm, such as production, order fulfillment, payment processing, or customer support. For each, map the people, applications, equipment, facilities, information, suppliers, and countries involved. Agree how long the business can tolerate a disruption and which services must be restored first. Identify dependencies shared across regions and test whether alternatives actually work.

03 Maintain a jurisdiction and obligations register

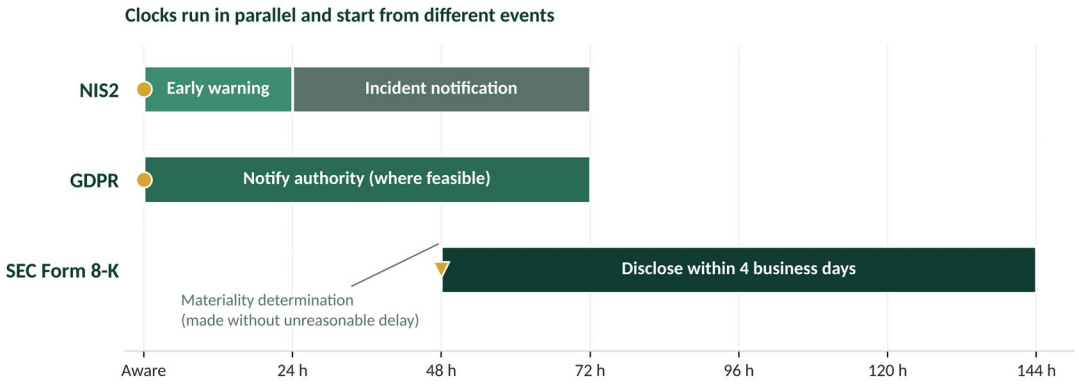
Legal and compliance teams should link each entity and service to applicable laws, regulators, contracts, reporting thresholds, deadlines, decision-makers, and notification channels. Record the event that starts each reporting clock. A single incident can trigger more than one obligation, and the clocks do not necessarily start together.

TABLE 2 **Examples of reporting obligations**

REGIME	TRIGGER	GENERAL TIMING
EU Network and Information Security Directive 2 (NIS2)	A significant incident affecting a covered essential or important entity	Early warning generally within 24 hours of awareness; incident notification generally within 72 hours. National implementation and sector rules matter.
EU General Data Protection Regulation (GDPR)	A personal data breach, unless unlikely to risk individuals' rights and freedoms	Controller notifies the relevant authority without undue delay and, where feasible, within 72 hours of awareness.
US Securities and Exchange Commission (SEC) rules	A covered public company determines an incident is material to investors	Generally within four business days after the materiality determination; the determination must be made without unreasonable delay.

© 2026 Tralphium, LLC · Author: Donald Marzullo

FIGURE 3 Reporting clocks for a single incident



Illustrative only. SEC timing counts business days from the materiality determination; the 48-hour start point is an example.

These examples have different thresholds and exceptions and are not a complete legal checklist. The relevant legal team should verify applicable law and contracts for each entity and incident. [5–7]

04 Apply and verify a global security baseline

A baseline is the minimum set of controls required across the enterprise. It should include strong authentication, restricted administrative access, timely security updates, inventories, protected logs, and recovery capabilities. Multifactor authentication requires more than one form of verification; phishing-resistant methods are designed to prevent attackers from reusing credentials captured through deceptive messages or sites.

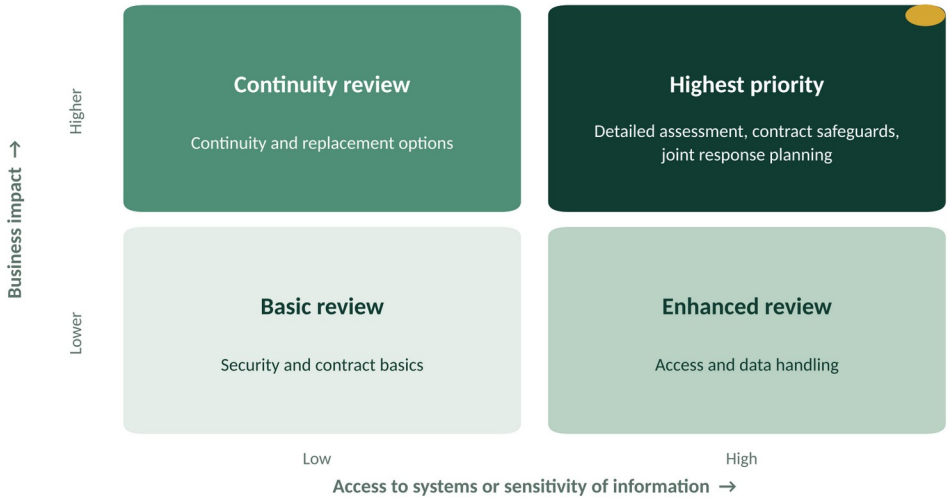
Restrict remote access to sensitive equipment, segment networks where appropriate, encrypt sensitive information, and protect backups from the systems they restore. Test recovery against business objectives. Document each exception with its reason, owner, temporary safeguards, and review date. The United States Cybersecurity and Infrastructure Security Agency (CISA) offers cross-sector performance goals that can help organizations prioritize basic controls. [8]

05 Manage suppliers by business impact

Review a supplier according to its access, the sensitivity of information it handles, and the consequences of its failure. Before contracting, identify subcontractors, assess security and continuity evidence, and define incident notification and cooperation expectations. During the relationship, review material changes and include critical suppliers in exercises. At exit, revoke access and address return or deletion of information. [9]

© 2026 Tralphium, LLC · Author: Donald Marzullo

FIGURE 4 **Supplier review priority**



This matrix is a starting point. Consider subcontractors, geographic concentration, and the time needed to replace a provider before setting a final priority.

06 Govern international data flows

Map where sensitive data is stored, accessed, processed, backed up, and shared, including remote support and incident investigations. For each flow, identify the purpose, data owner, recipients, locations, and applicable legal requirements. Limit access, apply appropriate encryption, and define retention and deletion practices.

For personal data transfers outside the European Economic Area—the European Union plus Iceland, Liechtenstein, and Norway—European rules provide mechanisms including adequacy decisions and standard contractual clauses. An adequacy decision recognizes a destination's level of protection for the scope covered by the decision; standard contractual clauses are approved contractual safeguards. Depending on the transfer, an assessment and additional protections may be needed. Review requirements with qualified counsel. [10]

07 Prepare people and rehearse response

Maintain primary and alternate contacts across time zones, clear escalation paths, external specialist arrangements, and an alternative communication channel. Train employees in their working languages and make it easy to report suspicious activity. Finance teams should practice verifying payment changes; procurement teams should know how to escalate suspicious supplier messages; facility teams should know how to report unusual equipment behavior.

© 2026 Tralphium, LLC · Author: Donald Marzullo

RECOMMENDED EXERCISE

Exercise a scenario involving a compromised supplier account, disruption in one country, and possible exposure of personal information in another. Record when teams learn of the incident, assess reporting requirements in parallel with the technical response, preserve evidence, and communicate confirmed facts and uncertainty. Test restoration before declaring recovery complete.

NIST recommends integrating response and recovery into broader cybersecurity risk management. [11]

08 Measure outcomes and improve

Leadership reports should show whether essential services can recover and whether material risks are being reduced. Use measures with defined owners, scope, and evidence. Investigate gaps rather than relying on a single score; set targets based on business risk and existing capability.

TABLE 3 **Executive dashboard template**

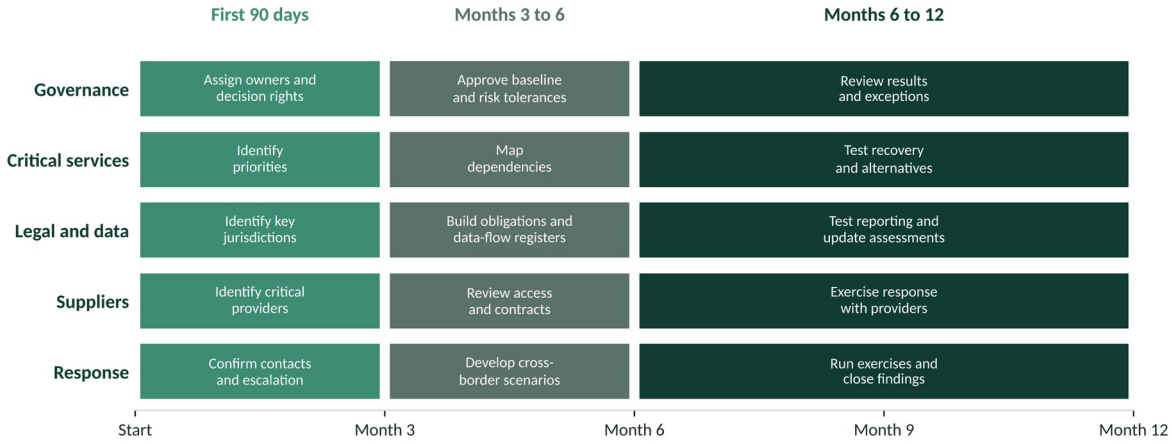
MEASURE	CURRENT	TARGET	OWNER
Critical services with a successful recovery test			Continuity
Critical suppliers with a current assessment			Procurement
High-risk vulnerabilities overdue			Technology
Material exceptions past review date			Risk owner
Exercise actions completed on time			Security

Blank template. Populate the Current and Target columns with verified organizational data; no figures are implied.

© 2026 Tralphium, LLC · Author: Donald Marzullo

Implementation roadmap

FIGURE 5 **Twelve-month implementation roadmap**



The roadmap is illustrative. Sequence and timing should reflect the organization's size, existing capability, and obligations. Fund local implementation and assign owners to every material gap.

Questions for leaders

FOR THE NEXT BOARD OR EXECUTIVE MEETING

- **Q1** Which services would cause the greatest harm if unavailable, and have we tested their recovery?
- **Q2** Where do multiple services rely on one provider, identity system, location, or communications route?
- **Q3** Can we identify affected entities, jurisdictions, customers, and data quickly during an incident?
- **Q4** Which local exceptions and supplier risks remain unresolved, and who owns them?
- **Q5** Can decision-makers communicate and act if normal systems are unavailable?
- **Q6** What did the latest exercise reveal, and which corrective actions remain open?

Conclusion

International cybersecurity depends on knowing how the business operates and where it is vulnerable to disruption. Start with critical services, map their dependencies, apply proportionate controls, and rehearse decisions with local teams and suppliers. Repeat the process as operations, providers, threats, and legal requirements change.

© 2026 Tralphium, LLC · Author: Donald Marzullo

About the author

Donald Marzullo is the founder of Tralphium, LLC. His career spans national security, government contracting, and federal executive support, including global operations, international partnerships, and complex negotiation, with professional experience in more than 100 countries across EMEA, Asia, and North and South America. He holds a JD and the CISSP and PMP credentials.

Sources

[1] **Maersk interim report, 2017**
https://investor.maersk.com/static-files/0ed2b2c8-518c-48ce-b009-c7b06308ad71

[2] **Maersk annual report, 2017**
https://investor.maersk.com/system/files-encrypted/nasdaq_kms/assets/2018/04/25/13-00-21/A.P._Moller_-_Maersk_Annual_Report_2017.pdf

[3] **UK National Cyber Security Centre, disruptive cyber activity**
https://www.ncsc.gov.uk/news/disruptive-cyber-activity-highlights-risk-from-internet-exposed-systems-and-edge-devices

[4] **NIST Cybersecurity Framework 2.0**
https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final

[5] **European Union NIS2 Directive**
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

[6] **European Data Protection Board, data breaches**
https://www.edpb.europa.eu/sme/assess-the-risks/data-breaches_en

[7] **SEC, cybersecurity disclosure**
https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-disclosure-20231214

[8] **CISA, cross-sector cybersecurity performance goals**
https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

[9] **NIST, supply-chain risk management guide**
https://csrc.nist.gov/pubs/sp/1305/final

[10] **European Data Protection Board, international data transfers**
https://www.edpb.europa.eu/sme/be-compliant/international-data-transfers_en

[11] **NIST, incident response recommendations**
https://csrc.nist.gov/pubs/sp/800/61/r3/final

DISCLAIMER

Regulatory information reviewed October 29, 2026. This paper provides general guidance, not legal advice. Requirements depend on the organization and circumstances and should be verified with qualified advisers.

© 2026 Tralphium, LLC · Author: Donald Marzullo

Tralphium $^{3}_{2}$He
STRATEGIC ADVISORY

Tralphium, LLC
Washington, D.C. metropolitan area
www.tralphium.net

Cybersecurity Across Borders: Best practices for international business leaders

Written by Donald Marzullo. © 2026 Tralphium, LLC. All rights reserved.

