Security through dependable workflows & advanced tools

by Rob Preston, *Senior Technical Sales Engineer, GTMaritime*

Shipping has always been pragmatic. If something works, it stays. If it fails, people route around it. That instinct has served the industry well for decades, but in today's increasingly connected environment, it's creating a new – and often overlooked – cyber-security risk.

Modern vessels are no longer isolated systems. They are part of a constantly connected operational network, exchanging navigation data, compliance reports, maintenance updates, and business-critical information between ship and shore. With the rise of VSAT, LEO connectivity, and hybrid communications, expectations around digital performance have increased significantly. At the same time, cyber threats targeting maritime organisations continue to grow in frequency and sophistication. In this environment, the reliability of data transfer is no longer just an IT concern; it's a fundamental part of cyber resilience.

A hidden failure mode

Consider a familiar scenario: a vessel is scheduled to receive a critical software update. The connection is unstable, though. The transfer starts, stalls, resumes, and eventually appears to complete. There is no clear confirmation of integrity. The crew assumes the update is done. Later, it becomes clear that the files were incomplete or corrupted. The process is repeated. Eventually, under time pressure, a technician arrives in port with a USB drive to 'just get it done.' Nothing in that chain feels like a failure. In fact, at each step, the system 'nearly worked.' In cyber-security, that is often more dangerous than something that fails outright.

When a transfer fails completely, it's visible. It triggers investigation and resolution. When it nearly works, it creates a pattern of behaviour. Crew begin to compensate. Files are re-sent manually. Processes that should be automated become dependent on human intervention. Physical media reappears because it feels more predictable. Over time, these workarounds become normalised. This is a hidden failure mode in maritime IT. It does not present as an incident. Rather, it presents as friction; and friction drives people to bypass controls.

Fragile necessity

The result is a gradual erosion of the security posture. Files are copied locally to 'be safe.' Policies are quietly ignored to meet operational deadlines. Patching is delayed because transfers cannot be trusted. Data is assumed to be complete when it is not. None of these actions are malicious. They are logical responses to unreliable systems.

USB usage is an obvious example of this dynamic. Despite years of investment in cyber defence, removable media remains widely used across fleets. Not because organisations are unaware of the risks, but because it solves a practical problem. When digital delivery is slow, unreliable, or unpredictable, physical transfer feels dependable.

However, that convenience comes with significant exposure. USB devices introduce a well-documented malware vector. They bypass network-based controls. They often lack proper audit trails. In regulated environments, this creates compliance challenges alongside security risks. Frameworks such as the International Maritime Organization's cyber risk management requirements and TMSA increasingly expect demonstrable control over data flows. Physical media makes that harder to achieve. The issue is not negligence; it's a necessity created by fragile systems.

Reliability vs pilling up (in)visible costs

This is why automated, encrypted, and integrity-checked transfer should be viewed not as an IT enhancement but as a core risk control. Reliability is cyber-security's quiet sidekick. It determines whether controls survive real operating conditions. A perfectly designed security policy is irrelevant if the underlying system cannot deliver updates consistently. If patches do not arrive, vulnerabilities persist. If training content fails to reach vessels, awareness degrades. If logs and reports cannot be transferred reliably, visibility is lost. The industry is not short of data; it lacks dependable delivery thereof.

Meanwhile, digitalisation on board continues to accelerate. E-navigation systems, performance monitoring tools, compliance platforms, and remote support solutions all depend on the continuous movement of data. Each additional system increases reliance on stable and predictable transfer mechanisms. More connectivity has not reduced this dependency – it has amplified it.

This creates a compounding effect. As fleets scale their digital capabilities, any weakness

Photo: Canva

in data transfer becomes more significant. What was once an inconvenience becomes an operational risk. There is also a clear commercial dimension. Unreliable transfers increase the workload for both the crew and shore teams. IT departments chase failed deliveries instead of focusing on higher-value security tasks. Delayed updates can lead to downtime or degraded system performance. In some cases, incomplete or corrupted data can impact operational decision-making. These are not always visible costs, but they accumulate quickly across a fleet.

No drama!

The human layer is critical in this equation. Crews operate in demanding environments, often under fatigue and time pressure. They are not cyber-security specialists, nor should they be expected to manage complex data workflows. Systems that require constant monitoring, retries, or manual intervention increase the likelihood of errors; those that work quietly in the background reduce it. In maritime, 'user-friendly' does not mean intuitive interfaces or better dashboards. It means minimal interaction. The most effective systems are those that remove the need for human involvement altogether.

This is where the concept of 'data transfer without drama' becomes important. It is not a marketing phrase; it's an operational requirement. Reliable transfer should be invisible. Regardless of connectivity conditions, files should move automatically, securely, and completely. Interruptions should be handled seamlessly. Integrity should be verified without user input. Audit trails should be available without additional effort.

Achieving this requires a shift in how solutions are evaluated. Buyers often focus on features, performance metrics, or cost. Less attention is paid to behaviour under real-world conditions, particularly when vessels are offline or operating with limited bandwidth. Before signing the next technology contract, organisations should ask a simple question: what happens when the vessel is offline? If the answer is unclear, it's not resilience that's on offer; it's a cat-in-a-bag special in the form of future workarounds. A yieldless venture with a headache ROI…

A resilient approach to data transfer typically includes several key principles. Store-and-forward capability ensures that data is not lost during connectivity gaps. Automation removes the need for crew intervention. Encryption protects data in transit. Integrity checks confirm that files arrive complete and unaltered. Resume functionality allows transfers to continue without restarting from scratch. Comprehensive logging provides visibility and supports compliance. None of these elements are new in isolation. The challenge is ensuring they work together consistently in the maritime environment, where connectivity is inherently variable.

Secure ≠ complex

As the industry continues to digitise, the margin for error is shrinking. Cybersecurity is no longer defined solely by firewalls and endpoint protection. It is shaped by the reliability of everyday processes. The most secure environments are not necessarily the most complex. They are the ones where systems work so consistently that nobody feels the need to bypass them.

This is particularly important as regulatory pressure increases and cyber risk becomes more visible at the board level. Organisations are being asked not just to implement controls, but to demonstrate that they work in practice across entire fleets operating in inconsistent conditions. Reliability is what turns policy into reality.

In shipping, security is built as much through dependable workflows as through advanced tools. The most dangerous data transfer is not the one that fails; it's the one that nearly works, because that is the one people learn to live with. ■