The World's Largest Circulation Marine Industry Publication • The Information Authority for the Global Marine Industry since 1939 • Number 4 Volume 80

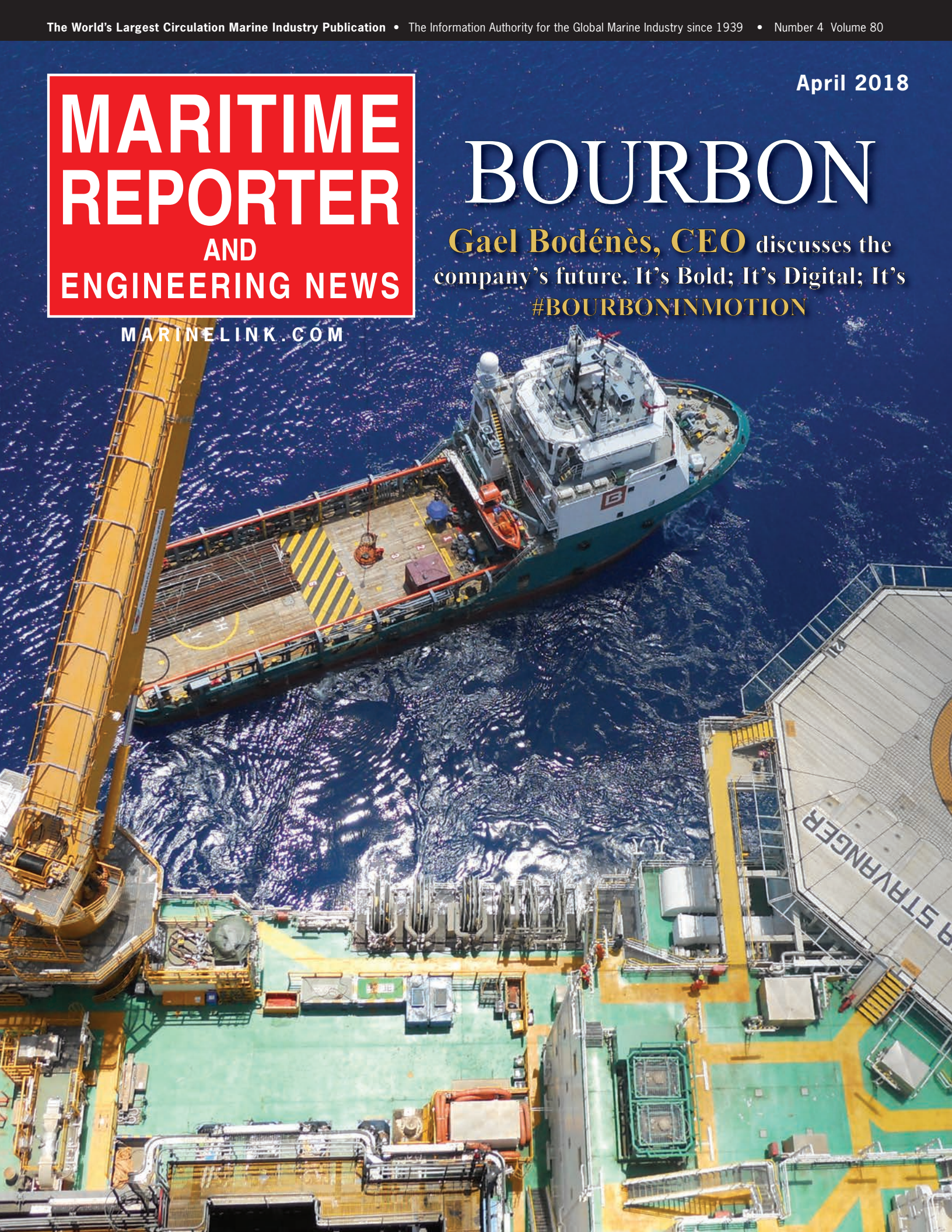
MARITIME REPORTER AND ENGINEERING NEWS

MARINELINK.COM

April 2018

BOURBON

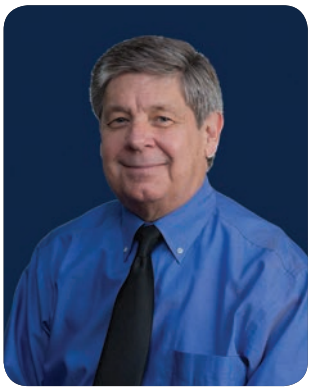
Gael Bodénès, CEO discusses the company's future. It's Bold; It's Digital; It's #BOURBONINMOTION



Cyber Security

What's Your Approach?

It is time to move toward a quantitative approach *that provides deeper understanding of individual risk elements observed in marine operating systems*



About the Author

Rick Scott, PE, BSIE, ME, is ABS Senior Technical Advisor who has worked in academia, high-tech manufacturing and the maritime industry for more than 45 years

Increasing connectivity in complex maritime operating systems is escalating the potential impact of cyber-related incidents and complicating the task of defending against them. Traditional methods for assessing cyber risk provide inadequate guidance for applying limited security resources.

Currently, available risk assessment methods are largely qualitative. Even so, these methods do provide the current foundation for risk management plans, on which owners and operators base programs to identify, protect, detect and recover from cybersecurity breaches. Building on that model, it is time to move toward a quantitative approach that provides deeper understanding of individual risk elements observed in marine operating systems, and provides owners with engineer¬ing "knobs to turn" to reduce them.

One of the things **ABS' research with the Stevens Institute** *discovered was that the nature of maritime risk within cybersecurity is not well defined or understood.*
Nor is it particularly well managed.

Reprinted with Permission from the April 2018 edition of Maritime Reporter & Engineering News - www.marinelink.com

The most common equation used to represent cyber risk is: Risk = Threat x Vulnerability x Consequence. This equation has proven useful for practitioners insofar as it has helped analysts intuitively understand that risk has three constituent elements, and infers that by removing one of these elements, risk can be reduced. But this formula is less an equation, in a mathematical sense, than a reference model for understanding the nature of cybersecurity risk. Its three elements largely are difficult to measure and are problematic when trying to engineer and/or calculate a cybersecurity solution. For the modern maritime risk practitioner, the core challenge is to create a model that defines cyber risk so it can be counted, measured, computed and modeled for maritime operating systems.

ABS recently collaborated with Stevens Institute to research this problem for the maritime sector and redefine the equation in terms that are countable, observable and easily understood. One of the things our research with the Stevens Institute discovered was that the nature of maritime risk within cybersecurity is not well defined or understood. Nor is it particularly well managed.

The result is a new model that helps owners proactively gain control over cybersecurity risks.

These risks in turn drive specific requirements, engineering decisions and resource commitments. The model focuses on identifying solutions that are computationally engineered, highly detailed and in context with the risks to be managed.

Effectively, it places the controls for responding to cyber risks back into the hands of the asset owner.

Shifting industry cyber risk practices away from more traditional defensive methods to a measurable process will require the industry to change the conversation, but most importantly it also will require a change in how risk practitioners think about risk.

To represent 'Consequence, Vulnerability, and Threat' as calculable elements of a risk equation for operating technology, we replaced them with the concepts of 'Functions, Connections, and Identities' (FCI), respectively.

'Functions' allow the crew to maneuver the vessel or perform its mission, which can be anything from drilling oil, to carrying people and cargo, or combinations of each. In the FCI risk equation, they represent systems that a cyber attacker would seek to control or defeat: steering, location monitors, propulsion systems, communications, anything to serve their purpose.

'Connections' represent, in relation to maritime operating technology, how the functions communicate with one another, to shore, to satellites, to the Internet, etc.

Within each connection is a 'node', the point through which a cyber incursion gains access.

'Identities' are either a human, or a digital device. Replacing Threat with Identity allows threats to be counted, a breakthrough concept for advancing maritime risk calculation.

In the context of the FCI model, a threat has to have an agenda. These can range from lack of awareness of cyber risks to unintentional behaviors – "I'm not going to adhere to company rules and perform my duties in a secure way" – or actions such as the hijacking of navigational systems to steal or destroy a vessel, or other acts disruptive to normal operations, typically for monetary gain.

The quantitative data from the Functions, Connections and Identities are then counted and used to populate a worksheet that builds a Risk Index to demonstrate how specific FCI alterations would change the relative risk of each system's configuration.

The process described here is simplified, but the Risk Index ultimately provides a quantitative view of the relative risk associated with the architectural design of individual systems onboard the vessel. That is something that has been missing in the maritime cybersecurity space.

The FCI method determines whether Connection nodes (the access points) are adequately protected, and whether or not the asset owner has controlled the Identities of those who have been provided access to nodes and restricted areas within the vessel control system architecture.

The Index illustrates each component's contribution to the overall risk. Based on those individual risk contributions, for example, the owner can redesign a network architecture to re-engineer how the system is being accessed, either through human-machine interfaces, cell phones, thumb drives, or connections to the Internet.

This new approach allows the owner to take a fleet-wide view to determining the relative risk associated with each vessel based on the way its digital system is designed, the way people are allowed to access it, and the way the nodes, or access points, are protected.

ABS delivers a risk index calculated through the FCI approach, which is a number that represents the relative level of risk inherent in the design and operation of the digital system on the ship. It helps owners to decide where to deploy their often-limited cyber-defense resources.

There is an old adage in industry: you can't manage what you don't measure. As the maritime industry continues its march towards auto¬mation, companies that can measure and manage cyber risk will be better positioned to tackle challenges in the new digital era.

As an industry, the ability to measure cyber risk will become a core foundation for operational efficiency and safety.

REDUCE YOUR CYBER RISK

Offshore and marine assets are seeing greater levels of automation and complexity. With more complexity comes increased system vulnerability and potential operational and safety impacts. ABS' practical methodology calculates marine and offshore Operational Technology (OT) cyber risk.

The ABS CyberSafety® program identifies risks and increases awareness of and protection from OT cyber threats to:

- Minimize productivity loss
- Lessen financial impact
- Optimize security budgets

Learn more about our practical approach to reduce your cyber risks.

ww2.eagle.org/cybersecurity

LEADING THE FUTURE