THE BUSINESS CASE FOR CYBER RISK MANAGEMENT IN THE MARITIME DOMAIN

A White Paper
Provided by Chris Coyle
of RiskSense,
A NMLEA STAR Product

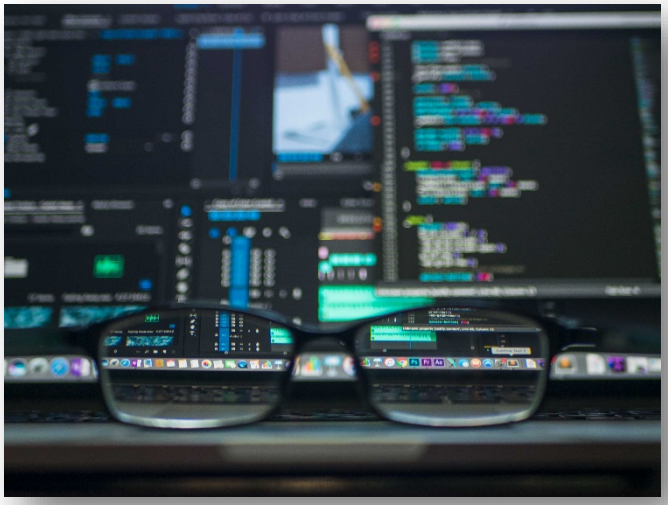
RISKSENSE
TRANSFORMING CYBER RISK MANAGEMENT

NATIONAL MARITIME LAW ENFORCEMENT ACADEMY

The Business Case for Cyber Risk Management *in the Maritime Domain*

Among the many opportunities to reduce costs related to managing cyber risks across an organization, managing the costs of cyber risk insurance is emerging as another significant advantage of RiskSense. According to the *Economist*, *"Demand for cyber-insurance is growing fast. Satisfying it will pose great challenges for insurers."* See Insurance section on page 4 below.

Synopsis: Organizations are re-considering their cybersecurity strategy due to several factors;



- ✓ The financial and legal consequences of a breach are increasing.
- ✓ The acceleration of cyber threats, including the growing pace and scale of attacks mean organizations cannot stand still.
- ✓ The steady growth of the digitally connected enterprise (e.g. IoT), also known as the "Attack Surface" is dramatically increasing cyber risk.
- ✓ Increasing end-point, perimeter security tools, or additional compliance-based activities are often ineffective at reducing cyber risk, and
- ✓ Organizations are looking for business-case rationale to help drive better cybersecurity strategies.

With spending forecasts projecting global cybersecurity spending to exceed $124 Billion in 2019[1], the questions most often asked are: What should our budget priorities be? Hire or contract with cybersecurity experts? Purchase more scanners and cyber security software?

Implementing a cyber risk management program is emerging as the leading investment for a number of important strategic and business reasons. Cyber risk management is a proactive, predictive and preventative approach to managing the growing scope and sophistication of cyberattacks. This does not replace what you are doing now; it makes it more organized and effective. Also called "continuous adaptive risk and trust assessment ("CARTA") approach by Gartner, Inc., cyber risk management focuses on using data to prioritize your highest risk vulnerabilities and accelerate the remediation process.

[1] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

The Business Case for Cyber Risk Management *in the Maritime Domain*

Cyber risk management offers significant strategic advantages and represents compelling business case value. From direct savings associated with labor savings, the elimination of separate, often siloed solutions, and other cost savings, the **RiskSense platform offers a clear business case value**. Add to that the indirect savings such as reduced cost of cyber standards compliance, better management of 3rd party supplier cyber risk and potentially a reduction in cyber insurance premiums, and the value of RiskSense presents a solid business case and return on investment considerations.

Using the budget elements of labor savings represented by a Full Time Equivalent/(FTE) cost savings per year, and the elimination of costs associated with software programs and services to support the cybersecurity management process, one can estimate a range of direct savings depending on the size of the organization.

- For smaller organizations the direct savings can amount to one or several FTEs or up to $100,000 – $150,000 in annual savings.

- For large, multi-unit enterprises that may comprise divisions and span states or continents, the direct savings can multiply based on the reduction or elimination of labor and end point solutions associated with managing the remediation process across groups. Direct savings can approach the $200,000 – $300,000 range.

Similarly, when organizations consider the in-direct costs of the FTE activities associated with cyber security standards compliance, the screening and cybersecurity management of 3rd party suppliers and partners as well as the value related to reducing the costs of cyber breach insurance or reselling cyber risk management services to customers, the indirect savings and value can add up an additional savings of 4 – 6 FTEs, and savings/new revenue in the $100,000 + range.

Direct Savings Summary: 2 to 6 FTEs/Year + Reduction in Spending for 3rd party tools & services.

This is accomplished through:

- Vulnerability management: Streamline and accelerate the review of scanner and other raw vulnerability data such as pen tests. Replacing a manual process of threat and vulnerability research to establish a priority list (often using paper-based spreadsheets and a yellow highlighter), RiskSense ingests, organizes and prioritizes this data. (Savings: up to 1 FTE/Year)

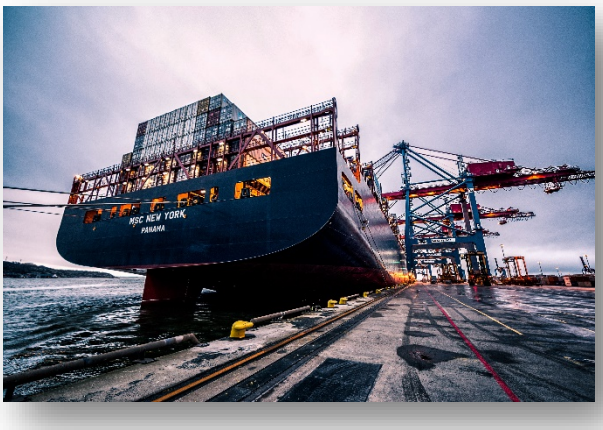
- Remediation workflow: Ability to tag, assign and manage the end-to-end remediation process, including capabilities to support faster and more effective use of remediation resources. In organizations where remediation actions are assigned to other FTEs across groups or divisions, these savings can scale accordingly. (Savings: up to 1 – 2 FTE/Year)

- Verification: Ability to track and verify the accurate, complete and successful remediation actions. (Savings: up to 1 - 3 FTE/Year)

- Reporting: Replacing manual report writing and/or the loading and management of data visualization software to communicate cybersecurity status and activities with the automated RiskSense RS3 score, executive dashboard and configurable report engine. (Savings: up to 1 – 3 FTE/Year)

- Reduction/Elimination of software programs and services: From data visualization programs and less comprehensive threat intelligence subscriptions to programs to manage internal and external penetration testing and cybersecurity assessment data, the RiskSense platform enables organizations to reduce their IT spend for what are often siloed programs that require constant FTE attention to operate. (Savings: up to 1 – 3 FTE/Year plus the cost savings from eliminating duplicative tools and services)

Indirect Savings Summary: 3 to 6 FTEs/Year + Services Savings & New Revenue Opportunities



This is accomplished through:

- Compliance: In addition to the CIO/CISO tasks related to vulnerability and remediation management, many organizations have additional personnel managing cyber and data security compliance reporting. From ISO and NIST to ITIL, PCI and many others (notably the EU GDPR regulations and similar federal and state statues currently being considered), organizations must collect and summarize the details of their cybersecurity actions and results. The RiskSense platform provides a ready source of current date data that can save months of FTE time. In addition to being continual, contextual and threat-adaptive compliance reporting becomes a by-product of the RiskSense platform in action. (Savings: up to 1 – 2 FTE/Year)

- Vendors & Partners: One of the main sources of cyber-attack is through 3rd party vendors and partners as evidenced by several nationally reported breaches that were introduced from connecting electronically with a supplier. Trying to lock down these digital connections that are often mission-critical to business and industrial workflows and value streams can be labor intensive. RiskSense can be used to streamline the assessment, prioritization and management of 3rd party cyber risks, often adding value to the 3rd party supplier. (Savings: up to 1 – 2 FTE/Year. Potential opportunity to charge 3rd party suppliers for the cyber risk reduction services.)

- Insurance: According to a recent article in the *Economist*[2], *"the need for robust insurance will only grow as companies become more reliant on computers hackers get more cunning and regulators take an increasingly din view of lax security".* The article goes on to describe other challenges in the cyber risk insurance industry, including the difficulty of pricing cyber risk insurance *"At the same, cyber-security risks are inherently tricky to price."*

  Many organizations are adding or increasing their insurance for cyber breaches. Most insurance companies use checklists, interviews and audit-type discovery to gather data for setting coverage and premium levels. A fully deployed and actively used RiskSense platform offers organizations a tool to demonstrate their improving cyber risk posture and their ability to streamline and focus the remediation process to minimize cyber risk. (In this case estimated savings may be speculative. However, there are likely cost savings related to reduced staff time managing the cyber risk insurance process and the potential opportunity to lower the cost cyber risk insurance premiums. FTE savings: $50,000 – $150,000 & Insurance Premium savings 10 – 25% or more?)

[2] https://www.economist.com/finance-and-economics/2019/01/26/the-market-for-cyber-insurance-is-growing

- Reselling Cyber Risk Management Services: Some organizations offer add on services for their customers that may include IT support, and cyber security services. Using the RiskSense platform, these organizations can extend and augment the value of their services by ingesting customer vulnerability data and providing access to their multi-client RiskSense dashboard to help them prioritize their highest risks and gain the advantages of RiskSense. (Potential opportunity to sell additional services to customers. $50,000 – $150,000)

Conclusion

Using the RiskSense platform can decrease the overall attack surface by 50% and security/IT teams greatly reduce the time to identify and analyze vulnerabilities and manage remediation actions by 90%. As the first cyber risk management tool that allows your organization to view the growing attack surface on a single pane of glass, RiskSense drives direct and indirect cost savings and value creation that is measurable and material. From senior management to IT staff managing remediation tasks on a daily basis, the RiskSense platform streamlines and focuses your resources and investments, enabling a proactive and preventative cyber security posture with an attractive return on investment.

Just look at what the experts are recommending; cyber risk management or Threat and Vulnerability Management ("TVM"*) offers compelling rationale for making it the priority for your 2019 cybersecurity budget.

According to the nationally recognized Gartner, Inc. (Gartner®), *Market Guide for Vulnerability Assessment*, June 19, 2018, while the cyber security assessment of traditional network-based and standard IT assets is generally supported by vulnerability assessment ("VA") vendors, the emerging areas of cloud, applications and mobile are often out of scope. Support for emerging applications which are connected to enterprise networks, varies widely, with coverage of cloud and mobile technology sporadic and immature. Notably, Gartner points out that VA buyers are increasing their focus on analytics and remediation prioritization (Called threat and vulnerability management or "TVM")

While some single-point VA solution vendors are beginning to add these capabilities, ***TVM vendors such as RiskSense can leverage the IT cyber end-point tools states already have in place.*** Gartner points out that the unique value TVM offers by using things like other forms of data such as threat intelligence on attacker activity and vulnerability use in malware, internal asset criticality, and other value-added capabilities to provide a better view of real risk for an organization to understand and prioritize cyber risks to proactively prevent breaches.

Gartner explains that TVM:

*"**[a]lso helps significantly in the prioritization work** that falls not on, security practitioners, but, instead, IT operations folks who have to do the last-mile leg work who do the patching and dealing with the consequences. **The benefit is that security teams are presented with what is a generally smaller list of higher-risk issues**. **These can then directly map into tools that security teams often have already deployed and have been managing** for well over a decade now, such as intrusion detection/prevention systems (IDPSs) and/or web application firewall (WAF) systems, to help with configuring these compensating controls."(Emphasis added)*

Contact us for a no-obligation Cyber Risk Assessment

For more information: Info@nmlea.org
Contact Chris Coyle directly at cbcg@risksense.com or 401.524.7818
RiskSense is an NMLEA STAR Product | www.risksense.com