Proactive Cybersecurity Risk Management

The importance of governance and strategy at the second line of defense

EMERGENT

Proactive Cybersecurity Risk Management

The importance of governance and strategy at the second line of defense

About Emergent

We help organizations “See Around the Corner” through a combination of professional services, and our Instinct Engine™ risk-quantification technology.

Through our products and services, you have a clear risk-based approach to find, assign responsibility for, and respond to cyber risks. We were established by leaders in the US Government and banking sectors to address today’s emerging Digital Risk Management challenges.

CONTACT
Emergent Network Defense
1133 15th Street, NW
12th Floor
Washington, DC 20005

SeeTheSwarm@endsecurity.com

Earl Crane, PhD
CEO, Founder

Are you asking the right questions?

When we walk into an organization to assess their cybersecurity program or help them address a regulatory MRA, we start with one question;

What is your Cyber Risk Appetite?

This is a tough question every business leader now faces.

The reflexive answer to this question is always “none”, but that is too simplistic. The thoughtful answer is always “it depends”. The final answer is that risk appetite is nuanced and specific to your organization. Your statement of Cyber Risk Appetite should capture the business risks that are unique to your culture, values, technology, operations, and adversaries.

Let us share our five-step question model, and help you establish a Cyber Risk Appetite foundation for strong business today, tomorrow, and in the future.

Proactive Cybersecurity Risk Management

The importance of governance and strategy at the second line of defense

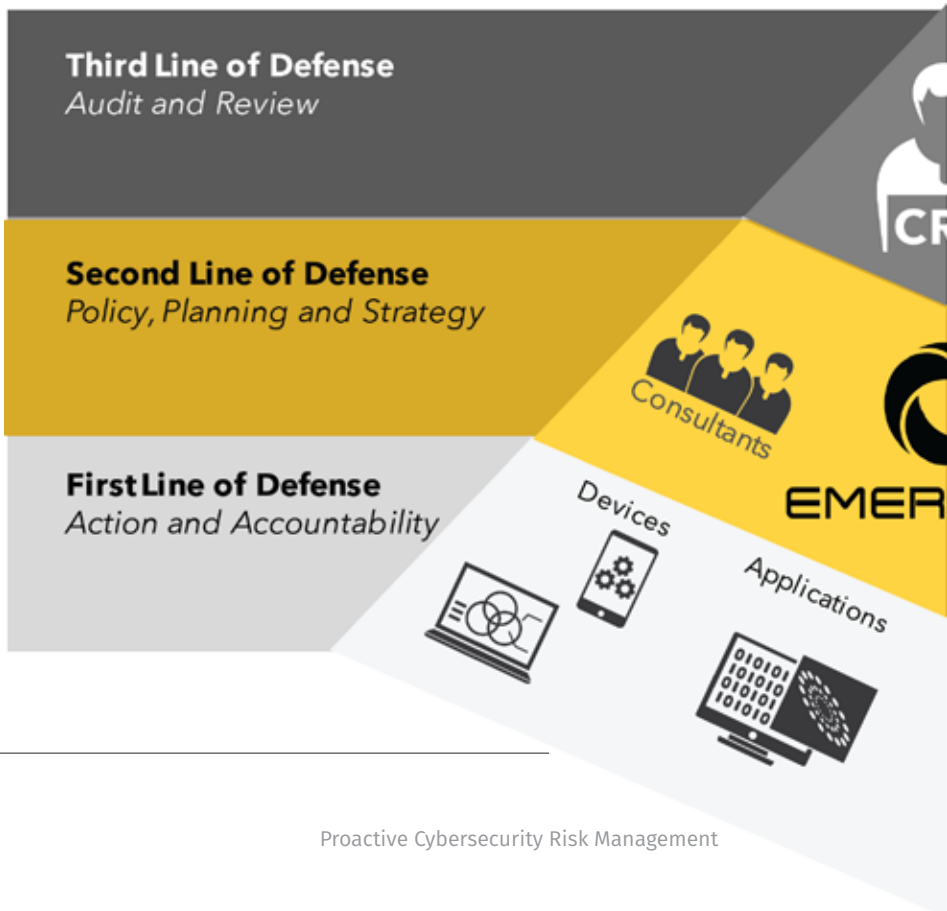
Strategy and governance are the most important starting points for cybersecurity risk management. You have to know where you want to go if you want to get there.

As cybersecurity leaders, you are constantly expected to recalibrate your strategy and defenses for a shifting threat profile and vulnerability landscape, all while operating under reduced budgets and increased scrutiny. Your defensive strategy must be both insightful, experienced, and grounded in factual data that changes daily. This requires strategic planning and a governance program that is informed by the daily onslaught of cyber threats and vulnerabilities, but one step removed to look at the impact on business consequences.

Three Lines of Defense

As companies become more interconnected and digitally-focused, Second Line of defense functions—CISOs, Risk Officers, and Executives—must monitor and manage cyber risk. First Line of defense cybersecurity and information technology tools are tactical in nature, and do not provide meaningful contextualized cyber risk quantification. To be successful, the second line of defense needs insight into the first-line trenches to make the difficult decisions necessary for cybersecurity risk management.

Without data, insight is hard and communicating the impact of cyber risk becomes impossible. As we all know, your job is not easy, and it's not getting any easier. The CISO and information technology staff have had little leverage in the business



decisions that create risk exposures. As these functions move to a second line function in some organizations, they need to be able to contextualize cyber risk in business terms, to motivate and shift responsibility to the lines of business creating risk in the first place.

First Line Cybersecurity Tools Do Not Quantify Risk

Second line functions need to answer:

- What is the next incident?

- How badly could it hurt the business?

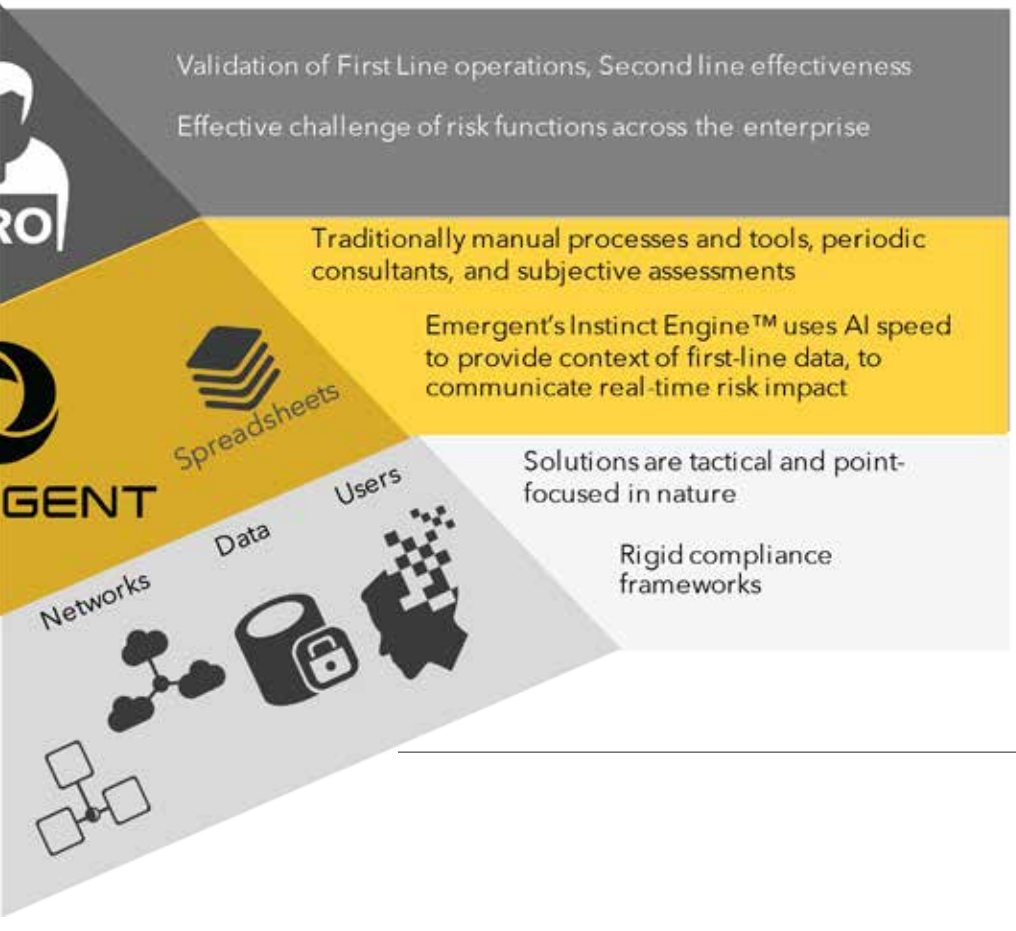
- What should we do to avoid or reduce the impact?

- Who owns the risk?

Many organizations already possess the data necessary to build a defensible cybersecurity ecosystem. The key information, however, is typically isolated in multiple compliance, systems management, or response silos. Risk metrics need tagged against major frameworks—like NIST CSF, FFIEC CAT, the Factor analysis of information risk (FAIR), or custom frameworks—to integrate and enhance existing reporting or governance structures.

A comprehensive cyber risk program is not only about compliance controls, it should be able to pull data out of an organization's data repositories, reducing or eliminating the need for constant data calls and consultant queries. This gets the second line the data they need for risk management, and lets the first line get back to the work of daily defense.

Providing a comprehensive reporting and rollup process, allowing enterprise governance and Cyber Risk Appetite to be communicated to business units is the key. As a result business line owners and other executives (CFO, CRO, COO) end up owning their cyber risk management responsibilities, just like they currently manage other existing business operations (quality, financials, schedules, etc). This empowers and enables all business lines generating cyber risks to also be responsible for managing those risks.



Emergent provides risk management and governance, in combination with a real-time integration platform that lets organizations build a new level of cyber risk management intelligence to empower executive governance, visibility and decision making.

EMERGENT

1133 15th Street, NW
Floor 12
Washington, DC 20005

www.endsecurity.com