SERVICE BRIEF

Cybersecurity Leadership Practice

Business-Driven Protection

Siloed cybersecurity management as a means to address current threats and adhere to audit or compliance standards is depleting resources, impeding efficiencies, and endangering vital data. NeuEon developed our Cybersecurity Leadership Practice to unchain organizations from the break-fix security mentality. Instead, we embrace right-sized security based on business need and risk profile.

Because we are comprised of C-level consultants with deep cybersecurity knowledge, we bring a skilled perspective on how information security champions a competitive edge. By addressing risk and adopting more flexible and ubiquitous cyber defense measures that support long-term goals tied to business drivers, we assist customers in reducing incidents that lead to loss of trade secrets, unanticipated costs, operational shutdowns, and reputational damage.

The NeuEon Approach to Cybersecurity

Information Security is not a problem to be solved by technology alone – it is an issue of converging business processes, risks, and the use of technology. This misunderstanding has led companies to operate with a break-fix mentality – whether internally or in partnership with external service providers. This cycle incites a false sense of security, resulting in limited long-term protection and greater risk exposure. Under this guise, assessments are performed to select technologies that advertise the ability to reduce identified risks.

NeuEon's cybersecurity advisement subscribes to a different school of thought in which we work to factor risk into executive decision making and work cohesively to implement changes that tie back to business goals for strategic business-security outcomes.

Our methodology is architected around People, Process, and Technology to establish:

- An understanding of cybersecurity responsibility at every level from board of directors down to administrative support
- A cybersecurity strategy that touches all aspects of an organization
- Technology that is selected based on thorough strategic analysis of business requirements and risk

NeuEon engagements are always tailored to the existing security posture and needs of an organization, utilizing a base of tools, strategic frameworks, as well as training and coaching methods. With risks and goals being dynamic, the path our customers take to holistic security is never linear and does not have a single endpoint.

Our fundamental goal is to guide organizations in redirecting cybersecurity efforts from reactive to proactive as an intentional mechanism to propel positive business outcomes.

Reputation is firmly rooted in trust. In the current climate, the onslaught of data breaches and other cyber risks are working to drive a wedge between businesses and their customers, suppliers, vendors, and even employees that do not have the tools or knowledge to protect sensitive data.

NeuEon knows that every company has a brand to uphold—that is why we work to protect hard-earned prestige from becoming a hacker's pawn.

People

Spanning Cybersecurity from Technologist to Executive

The cybersecurity skills shortage crisis is a widening business problem as organizations struggle to defend against increasing threats and comply with regulatory demands. The effects of the shortage are then exacerbated by:

- Inadequate training for cybersecurity professionals
- Lack of training for non-technical employees
- Limited or no internal cybersecurity staff
- Absence of knowledge and advocacy around impacts of improperly addressing risks

NeuEon's cybersecurity advisement is rooted in empowering all levels of an organization to identify with cybersecurity responsibilities.

EDUCATION

- Consult with executives to guide strategic business operations initiatives and security/privacy implications
- Transfer knowledge through training and mentoring of staff
- Guide technologists on practical implementation of security best practices and methodologies to address business problems
- Inform technologists on the connection between business problems/goals and security

COMMUNICATION

- Communicate with executives and board of directors using business appropriate language to inform cybersecurity decisions
- Act as liaison for audits and assessments
- Provide quarterly updates to business leadership and key stakeholders on possible business impacts from security trends and legal environment

VALUE

Working with all business levels, from executive to technologist, we establish our role as a trusted strategic advisor and cybersecurity lifeline. Using our position, we address the cybersecurity skills shortage head-on by providing actionable steps that aren't limited to prescribing additional certifications to technologists.

NeuEon inspires a culture of security by helping to recruit talent where necessary, employing more sophisticated and continuous training, and bridging the cyber/business gap to prevent reactive security decision making. By directly transferring our hard lessons learned, clients enjoy immediate access to cybersecurity excellence, saving them money, time, and trouble.

CYBERSECURITY LEADERSHIP PRACTICE

PEOPLE | PROCESS | TECHNOLOGY

SECURE PRODUCT DEVELOPMENT

With a focus on speed, "baking-in" security is viewed as an impediment to Agile software development, leading to reactive "bolting-on" methods. The lack of cybersecurity training for DevOps professionals compounds the issue, leading to an overall less secure product development.

When developing cybersecurity process, NeuEon works all the way through the business to include product development to blend Agile's benefits of efficiency and timely responsiveness with security.

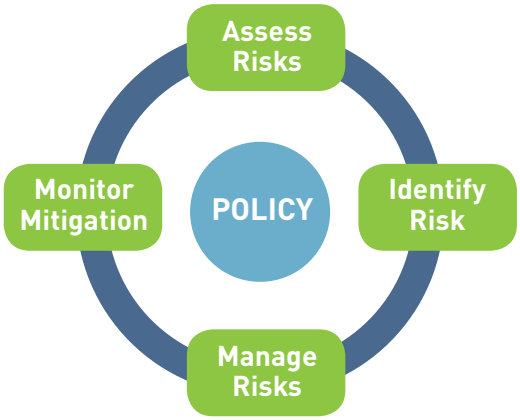
NeuEon's unique approach combines security mastery, process requirements, coaching and training, with the knowledge and expertise around Agile and High Performing Organizations. By marrying Agile software development and cybersecurity, DevOps seamlessly and proactively transforms to DevSecOps as the basis of reaching product development end-goals.

neu·eon

Process

Building the Business/Cybersecurity Connection

NeuEon's phased approach to building an Information Security Management Program (ISMP) is a repeatable process of assess, analyze, and recommend. At the beginning of the cycle we evaluate business criteria to determine the appropriate security framework that will act as the foundation to the ISMP.



Once the first wave is complete, the plan will address information security concerns, monitor and address risks, meet applicable regulatory requirements, and define the structure that will manage information security.

MANAGE RISK

RISK REGISTER

After the policy has been defined and a risk assessment is completed, we begin the management and mitigation of risk through a register that:

- Identifies all known risk
- Prioritizes risk based on potential impact to the organization
- Groups similar risks and associated tasks to form actionable projects

ACTIONABLE ROADMAP

Projects from the Risk Register feed into a Security Roadmap that acts as a blueprint to converge security and business actions. This can include:

- Yearly policy review
- Data access review and control
- Security awareness training
- Patch and vulnerability management
- Incident response
- Audit logging strategy

VALUE

NeuEon uses proven approaches to build comprehensive security programs that include tools, training, and expertise which reduce time and cost, as well as eliminate false starts.

Technology

Selecting Impactful Security Solutions

The impetus for cybersecurity technology selections should always be the transformation an investment will bring to the business. NeuEon's Technology Selection Process (TSP) provides a data-driven, disciplined approach that translates business need into specific requirements. Through the process, we can advise on cybersecurity solutions that support the health of the entire company, as well as its customers and other external stakeholders (partners, supply chain, etc.).

SECURE INFRASTRUCTURE

IT infrastructure is changing as the data of daily business moves outside the perimeter of the corporate network. With the volume and complexity of attacks continuing to rise, organizations must reconsider large capital investments – Will the expenditures overcome significant risks and hurdles businesses will face over the next 5-10 years?

Because NeuEon is not aligned with specific vendors, our recommendations are transparent, objective, and offer insight for organizations that struggle to recognize security-resource issues. By evaluating investments based on risks that place reputation, operations, and profitability in danger, technology selections are baked into business rather than applied as stop-gap controls.

RESULTS

Through assessment, coaching and training, and implementation of tools and processes, we strive for significant protection improvements based on industry frameworks. When we have completed our mission, an organization should have:

- Sound business spend decisions based on level of risk addressed
- A clear cybersecurity program that is linked to annual business strategy
- Alignment of employee skills with actionable cybersecurity practices
- A common understanding of risk within the organization
- An information security lifeline and knowledge base for continual strategic guidance

About **NeuEon**

NeuEon is a boutique consulting company focused on combining strategic technology transformation with practical implementation. For over a decade, the company has delivered measurable results for a wide roster of clients from start-ups to enterprise, with specialized services for the investor community. NeuEon's team of senior-level leaders with deep business and technology expertise apply proven methodologies and processes to enable clients to reach their objectives.

NeuEon, Inc. | 275 Grove Street, Suite 2-400, Newton, MA 02466 | 877.273.9200