N2Growth

Leadership In Cybersecurity

Originally Published On The Executive Hub:

Defining the position of the lead security person in an enterprise can be a challenging and sometimes confusing task. There are various job titles such as; Chief Security Officer (CSO), Chief Risk Officer, Chief Information Security Officer (CISO), V.P., IT Security, V.P., or Director of Information Security. Regardless of titles or functional position, the lead role in a security organization is expected to wear many hats and solve a myriad of strategic, operational and tactical problems.

Today's security leader must keep their pulse on a plethora of security initiatives. Below is a list of security initiatives that a security leader would either manage or have parallel impact upon within a business:

Data security	Vendor management	Budgeting & forecasting	Network systems security	Disaster Recovery (DR)
Application security	Identity & Access Management (IAM)	Vulnerability Management (VM)	Data storage	Business Continuity (BC)
Cloud enabled solutions – SaaS, IaaS, PaaS	Policy & controls development with implementation	Managing enterprise risk tolerance	Communicating to executives and board members	Human resource leadership
Incident Response Planning (IRP)	Multi-year security architecture planning	Audit management & support	Breach mitigation	Keep current with leading edge security solutions

Couple the above list of security initiatives with the below statements about the environments that security leaders are placed into, and you quickly realize a practical yet manageable shift is needed. Today's information security leaders are faced with:

1. Multi-vendor proprietary point solutions. This creates financially inefficient security architectures with increased vulnerabilities.

2. Technology aligned reporting structure. Security leaders are primarily reporting to the CIO. Security initiatives viewed primarily as technology solutions create misalignment with business requirements. This increases security spending costs.

3. Obtaining an effective security budget is a constant battle. If the security budget is measured

against a percentage of the IT budget, this creates an ineffective security posture for the business.

4. Black hats (criminals) don't care. Meaning, the bad hackers don't care if you are required to comply with a policy or law, nor do they care about your budget or resources. Time is on the side of the black hats – they only have to get lucky once.

5. Historically, security teams have been built in vertical silos. This enhances miscommunications and weakens trust across lines of business.

The new leader in information security must be envisioned as a leader integrator. This person accepts the responsibilities and accountabilities of the position but leads and manages with a higher order of thinking. The position requires an individual that can zoom in on technical discussion to solve tactical problems while comfortably collaborating and communicating with top executives. Security leaders today should be viewed as change agents, culture builders, transformers, visionaries yet able to keep their fingers on the tactical pulse of the enterprises security posture. Their position relative to the enterprise should have transparency to the executive team. The ability to present security information to direct reports or during a board meeting at a level understood by the audience is of vital importance to the overall risk management to the business. The new leader integrator for operational security is proactive with the following:

- Envisions security value horizontally – reaches out to other departments such as operations, finance, HR, sales and legal. Is a bridge builder across disciplines, departments and stakeholders
- Enhances collaboration through communication while building trust inside and outside the security organization
- Invests in security technologies that supports business objectives
- Actively listens while proactively accepting critique from subordinates, executives and board members
- Has a business and technology background and thinks as a strategic "holistic" thinker
- Constantly learns and stays abreast of emerging security trends, while transcending learning to the employees, organization or partners
- Is a persistent servant leader to others and helping individuals become leaders in their own right

The new information security leader understands that security transcends technology. Technology is the enabler to business yet security is the overarching business operations protection program. Tomorrow's security leaders will be required to effectively and efficiently integrate people, process and leading edge technologies to ensure a consistently relevant security posture for the business. This requires business acumen and the ability to think critically to solve complex problems. The time is now for security leaders of tomorrow to approach security as a business problem first, followed by the supportive skill sets, business processes and technologies required for securing the enterprise.