New Horizons
Computer Learning Centers

TODAY'S CYBERSECURITY REALITY IN 2018

Cybersecurity practitioners face challenges when it comes to having a security program that operates effectively. Sometimes it means looking at cybersecurity through the lens of capability and focus on the understanding of what risks there are. Here are some challenge areas that every business should evaluate when looking at their security program.

RISK MANAGEMENT

Businesses struggle with risk management, even those with a regulatory mandate to address risk management. Oftentimes risk management is not executed effectively or becomes increasingly difficult to implement correctly.

1. Risk management is often difficult to obtain and can be a moving target.
2. There can often be a disconnect between risk that an enterprise faces and the specific practices that are driven by regulatory compliance.
3. Compliance-driven efforts sometimes don't account for specific risks that enterprises may encounter.
4. Businesses are becoming more complex.

DUE DILIGENCE AND NEGLIGENCE

Due diligence is a critical (and legal) imperative that businesses need to invest time, energy and budget into, making sure all appropriate measures are taken to address security. However, standards may not align with industry norms. What that means is risk, not standard practice or industry norms, determines whether actions are negligent. Today's risk environment focuses not only on technology, but those responsible for it.

New Horizons Computer Learning Centers

TODAY'S CYBERSECURITY REALITY IN 2018

OPERATIONAL EFFICACY AND EFFICIENCY

Efficacy relates to whether security measures are sufficient and if they are working as intended, while efficiency looks at how well the process is working. Decisions about how to approach specific controls are made daily based on the organization. The time required to analyze is different, the resiliency of the process to employee attrition is different, potential for human error is different and the value returned for the money invested is different.

PRIORITIZATION

On the surface, the prioritization of which countermeasures to implement might sound like a direct risk management exercise, i.e., one invests in deploying the controls that provide the most risk reduction value. However, there are a few reasons why it can be significantly more complicated than this.

1. The increasing array of regulatory mandates, frameworks and guidance documents that are germane to any given enterprise can complicate prioritization.
2. Some implementation steps can address parts of multiple goals, such as, when the implementation of a risk mitigation measure is easier, if another task is undertaken first.

SECURITY OPERATIONS

The mechanics of security operations are another challenge area for enterprises, both internally and externally. Internally, obtaining adequate funding and shortage of appropriate skills can create challenges. Underfunding and staffing challenges are among the chief challenges facing security operations. Externally, attackers and defenders are in an ever-advancing arms race—attackers develop increasingly sophisticated tradecraft while defenders improve defense techniques.

Source: "A Risk-Aware Path to Cybersecurity Resilience and Maturity." ISACA.com, 2018.