Diversified™
IMAGINATION ENGINEERED

PERFORMANCE-BASED SECURITY

BEST PRACTICES GUIDE

Building and sustaining a resilient enterprise physical security practice

In today's fast-paced and constantly evolving global market, ensuring the safety of your organization's critical data is no doubt a high priority. However, firewalls won't stop an intruder from gaining physical access to your business, and it's just as important that your physical assets are as equally secured as those in the cloud.

Physical security is the first line of defense against unwanted breaches to your enterprise, but with rapidly advancing technologies, vendor and manufacturer consolidation, and increasing internal organizational complexity, selecting the right solution and provider can prove to be a daunting task.

Evaluating all options and charting the course for sound foundational solutions that are capable of evolving as your business needs change requires more than just product education and industry experience. It requires insight into market direction and provider positioning. Additionally, variability in both internal and external risks to the success of your security program further intensifies the criticality of having a solid programmatic and technological approach.

Well designed and deployed solutions that enable security and business practices are the result of an intentional and well-informed process. This methodical approach provides a comprehensive roadmap, positions your security organization to drive improvement, and delivers exceptional value to your overall organization.

ONE | **KNOW YOUR THREATS, UNDERSTAND YOUR RISKS**

"You do not achieve victory by defeating your enemy but rather by defeating your enemy's strategy." – Sun Tzu

- Effective security is designed in layers
- Identify key assets and high risk, high vulnerability areas
- Talk to your internal people throughout your organization – a lot!
- Feedback from key areas of operations within your organization creates well defined knowledge of vulnerabilities, exposes areas of opportunity to add value to the overall organization and creates a culture of security
- Consider both traditional and non-traditional threats
- Increasingly, the focus on core systems revolves around "the Security of Security"! Who has accessed your systems? What data is being reviewed, exported, and made accessible to unapproved users?
- Identify key processes and process changes that need to be implemented first. Then begin evaluating and investing in technology solutions that will meet those needs.

BEST PRACTICE

Consider developing internal organizational security "champions" who inform your understanding of both traditional and non-traditional sources of security threats.

TWO | **PRIORITIZE YOUR THREATS**

Data Validated Concerns

1. Internal threats
2. External threats
3. Traditional threats
4. Non-traditional threats
5. Technological "weak links" such as poorly performing network infrastructure and decentralized, disparate systems
6. Identify high vulnerability, high asset people and locations
7. Compliance requirements for any regulatory demands that come from the business side

Key Criteria

1. Driven by business requirements, not vendor presentations
2. Of the technologies available, which ones are best suited for your organization?

Leverage Existing Technologies or Consider New

1. Begin with a thorough analysis of the business level requirements.
2. Assess your current systems:
    - Do they integrate well with advancing technologies?
    - Is the manufacturer or OEM in a growing market position?
    - Does my solution allow for open market competition for my business?
    - Can my current technologies evolve as business demands change and my processes evolve?
    - Is the best approach to support on premise systems or do resource or strategy constraints make hosted solutions appealing?

BEST PRACTICE

To build a technology roadmap guaranteed to provide the most value for the lowest long term total cost of ownership, evaluate threats in light of business demands and select market disrupting but financially sound solutions that lead the industry direction with regard to solving your specific problems.

BEST PRACTICE

The appropriate foundational system(s) allow for cost effective layering to build the appropriate technology ecosystem.

THREE | **MULTI-LAYERED APPROACH**

It is an industry-known best practice that effective security is accomplished using a layered approach. The key is to determine which technologies represent the appropriate layers for your organization's culture and business requirements. Here are some ways to determine how many layers your organization needs:

- Define your "perimeter" or area of interest you need to protect
- Understand your options—access control and video are foundational systems, but there are new "low-tech/high-tech" means of gaining efficiencies that can save you time and money.
- Which layers are appropriate for you will depend on the following key factors:
  - The nature of your building or campus environment
  - The culture of your organization
  - Severity of threat
  - Technological capabilities
  - Budget available

FOUR | **BUDGET**

Planning and designing a perfectly efficient, sound security solution is a great step toward taking your enterprise security program to the next level. However, no matter how much thought is put into a project plan, its implementation always comes down to one thing—whether or not your organization has the means to fund the solution you are proposing.

When evaluating how much to budget for your security program, consider the following:

- Your 1/3/5 year roadmap will identify the fitness of your current systems to accomplish your business goals and objectives
- Identify the best end result and implement in phases. Review feedback on program effectiveness at each phase.
- Determine whether OpEx or CapEx is the best model for you
- Quantify recurring costs
- Consider application lifecycles and allow for tech refreshes along the way with major updates about every 7 to 8 years
- Consider liabilities

BEST PRACTICE

Sound security investors recognize that decisions revolve around the level of risk to be mitigated for a prescribed financial investment.

Keeping the process simple in today's complex evolving technology and business environment is more difficult than it seems sometimes. Many of the industry's key foundational principles still apply, but what has changed dramatically are the environments we implement in, the project team and stakeholders involved, and the options available to accomplish your objectives.

- Process enables technology—identifying the most effective process is primary
- Threat translates to risk—identification of the threats that create risk your organization cannot afford drives monetary considerations
- Implementation of appropriate solutions involves a view to operational efficiencies to demonstrate the value your team brings to the overall organization

The unique design and culture of Diversified affords our clients unique value. Deep synergies within our Mission Critical Environments, Intelligent Technology Solutions and Electronic Security Solutions teams provide an unparalleled and comprehensive end-to-end view of an organization's security practice and ecosystem.

LEARN MORE & CONNECT TO YOUR DIGITAL FUTURE

diversifiedus.com