What Is PhySec?

- Physical Security consists of physical, logical and design measures which protect people, physical property and other assets from harm, unauthorized access, usage, tampering, and theft.
Why Is PhySec Needed?

- Physical Security is put in place to help prevent – more accurately, to deter – crimes of opportunity as well as safeguard life.

- PhySec can also complement mitigating business liability by applying controls to known areas of possible physical risk.
Characteristics of a Sound PhySec program

• Physical Security can consist of many different elements which directly or indirectly address areas of perceived risk.

• Common elements of Physical Security Programs include:
  • Deterrence
  • Active detection and monitoring
  • Delay progress of criminal or other unwanted behavior
  • Incident response to alarms, alerts or attacks
  • Recover business or operational status as quickly as possible following an incident
Characteristics of PhySec

• Deterrence
  • PhySec controls build in deterrence as preventative measure. Deterrence is the initial attempt to thwart unwanted behaviors to include criminal activities through out the facility(s) being safeguarded.

• Active detection and monitoring
  • Active detection and monitoring can be viewed as overt, or intended to be seen, and covert or concealed. Monitoring is designed to provide early warning of possible security events, evidentiary value used for criminal or civil proceedings.
Characteristics of PhySec

• Delay
  • Delaying controls help limit or slow the progress of a breach, compromise, attack or other unwanted behavior.

• Incident response
  • Recover business or operational status as quickly as possible following an incident.

• Recovery
  • Recover business or operational status as quickly as possible following an incident.
Security Requirements

• To ensure the PhySec program is adequate; initial requirements should be outlined in order to better understand where to prioritize resources, budget and time.
Security Requirements

1.) Determine applicable threats or risks.

- Identify applicable threats and risks associated with the organization to include proximity to the organization.

- Ensure risk assessments take into account:
  - Surrounding businesses
  - Local infrastructures
  - Geographic areas of interest
  - Local environmental conditions
  - Geopolitical climate
Security Requirements

2.) Assess vulnerabilities which could allow threats or risks to affect personnel or operations.

• Once threats and risks have been identified; investigate and understand how those threats and risks, if capitalized on, would affect the organization.

• Ensure PhySec controls are appropriate for the identified vulnerabilities.
Security Requirements

3.) Compile a list of assets with associated value

- List should indicate value, the value of the asset will be used in determining resources available. Life is of utmost value and inherently priceless. **Protection of life is THE top priority.**

- Value is not always a monetary figure. Value can include the organizations commitment to availability and critical services provided by the organization.
Security Requirements

4.) What if scenarios - Examine and plan for failures in the PhySec plan.
   • Determine what the impact will be when PhySec controls fail.
5.) Determine cost of security vs. actual cost of asset to be safeguarded
- Cost of PhySec controls aren’t always black and white.
  - Cost of equipment
  - Cost of installation
  - Cost of training
  - Cost of liability for not having or having enough PhySec in place
Security Requirements

6.) Ensure installation and maintenance considerations are taken into account.

• Installation of PhySec controls can itself introduce security gaps.

• Reliance on temporary PhySec equipment vs. long term equipment may save money initially but may incur extra expenditures to maintain for long periods of time.

• Evaluate short term vs. long term needs and plan accordingly appropriate installation and support contracts.
Security Requirements

7.) Ensure PhySec implementations are complementary to business operations.

- PhySec systems must adapt to the organization. Different times or shifts may have different PhySec requirements.

- PhySec should meet the organizations requirements while minimizing the impact on daily business.

- PhySec which is too overly cumbersome will not be utilized to the fullest by the organization.
Security Requirements

8.) Security should include seen and unseen measures which provide overall PhySec safeguards.

- PhySec which is seen provides an initial deterrent.

- Some deterrents are meant to be seen as to provide misdirection or obfuscate covert PhySec controls.

- Overt PhySec controls often times provide organizational employees with a sense of security.

- Covert PhySec controls should work in a complementary manner with overt controls.
Security Requirements

9.) Simplify PhySec controls in order to lesson human error.

• Ensure that staff and security personnel have sufficient training in order to safely and efficiently operate the organizations security apparatus.
10.) PhySec controls are a long-term commitment; ensure PhySec takes into account future growth.

- Take into account physical changes or additions to the organizations structure.
- Licensing considerations for PhySec software controls.
Changing The Mindset

- PhySec is the implementation of an organization's active response to areas of assessed risk.

- PhySec should not be a hurdle or roadblock, rather it should be used to help shape and modify behaviors.
Changing The Mindset

• Often times Information Security and Physical Security officers are seen as the office of “NO”. Implementation of appropriate PhySec controls which support the business and its customers is a critical balancing act.

• Too little PhySec exposes the business to elevated risks.

• Too much PhySec creates business obstacles which can impact productivity and profitability.
Incidents PhySec Should Address

- Incidents PhySec programs should address through logical, physical and design controls:
  - Policy / Procedure violations
  - Natural disasters
  - Rogue or trusted insider risks
  - Workplace violence
  - Unauthorized entry / Trespassers
  - Criminal acts internal / external
  - Industrial disasters
  - Civil disturbances
  - Terrorism
Case Study
Case Study – Large National Bank

• This stuff happens to the big guys as well…

• Services provided around the country
  • National branch and service location footprint
    • Retail and commercial services
    • Mortgage services
    • Merchant services
    • E-banking
    • Growth primarily through acquisition
Case Study – Large National Bank

“Great Candy” for attackers...

• Hard outer shell...Great Perimeter network security
  • Banner replacements for open ports
  • Outsourced web services to well known, SSAE16 backed companies
  • Proxy server in place for staff to utilize when connecting out
Case Study – Large National Bank

• “Great Candy” for attackers…
  • Soft, chewy center…Terrible internal and physical security
    • Open network between lines of business
    • Complete lack of physical security controls
      • Mortgage service centers in particular
      • Examples to follow
Case Study – Large National Bank

• Physical controls were leveraged against the bank’s information
  • To “great” results for the attacker
    • We infiltrated EVERY physical location without breaking a sweat
      • Branches included
    • We were able to gather client and employee data right from the desks of the information owners
      • Offered lunch in one facility
  • Terrible results for the bank…
Q&A...
THANK YOU!
Questions?
edward.vasko@tvrms.com
Office: 480-840-1744
info@TVRMS.com
http://www.TVRMS.com