Infinova
The Integrator's Manufacturer

White Paper

How to Perform a Site Security Survey and Build a Risk/Vulnerability Matrix

Risk management is not about eliminating risk but managing it and being prepared to deal with security failures through resiliency. A site security survey and a risk/vulnerability matrix can help security managers reach better business decisions relative to existing and new security video technology.

Security technology is just one part enterprise risk management, even though an important part. Examining the organization from outside in and focusing on possibilities is a healthy exercise. Such a risk assessment has to be creative and subjective. But it is not the end point. Creating and constantly evolving a risk/vulnerability matrix adds the ability to prioritize threats while choosing or upgrading technology that will prove more effective both in terms of cost and loss prevention.

Such exercises also bring personalized business intelligence to the job of the chief security officer or security director. This is especially helpful today with the ascent of security video and the challenges of analog and digital coexistence while security transitions to digital video surveillance.

When it comes to a site security survey and producing a risk/vulnerability matrix, CSO Terry Jones and Helena Smith, his second-in-command, who work for a mid-sized enterprise, will seek outside advice to help bring a fresh viewpoint to the assignment. Jones and Smith have been part of this series of white papers as they face the specifics of technologies and the demands of the business.

A first report in this Infinova white paper series examined, in an overview way, the coexistence strategy at the heart of a cost-effective move from analog to digital security video. That white paper also overviewed the impact on infrastructure including sharing the enterprise data network, bandwidth and compression schemes. A second white paper explored cameras – analog to IP-based as well as megapixel and high definition. The third white paper examined benefits and ways that fiber optics enhances the operation and business bottom line of surveillance solutions. A fourth white paper looked into the myriad storage options and ways to determine which are best for the needs of the enterprise. These previous white papers are available for download at www.infinova.com

Risk Management Is a Broad But Valuable Concept

Over coffee, Helena shared with Terry information she recently gained from a seminar on enterprise risk she attended with the firm's risk manager and information security manager, which was based on materials from PricewaterhouseCoopers. She learned that convergence or fusion of security risks is a broad term which covers the multiplicity and interdependence of a variety of risks which the business faces.

It requires a response which brings together all those dedicated to the security of the organization to assess collective corporate risks, risks that when looked at in isolation can increase the probability of the risk materializing. Many of the conventional security risks are viewed in isolation. These risks may fuse or overlap at specific points during the risk lifecycle, and as such, could become a blind spot to the organization or individuals responsible for security. Convergence of security risks is important because those blended or converged risks that pose the greatest risk to people and organizations are often unknown. This includes converged security risks from common and complementary operating processes in addition to more commonplace threats. To protect our people, our businesses and our assets, we need to keep ahead of those who attack us and work with internal and external forces to identify and understand those potential blind spots that could cause the business most damage, Helena advises Terry. This makes the case for regular site security surveys leading to changes in a risk/vulnerability matrix.

Author
Mark S. Wilson
Vice President, Marketing
Infinova

There's a diversity of security threats.

- Accidents involving employees and visitors
- Natural disasters
- Data loss
- Fraud
- Intellectual espionage
- Vandalism
- Threats to people
- Physical theft
- Brand and reputation attacks

The multiple and complex merging of risk is causing organizations to rethink their security risk strategy. Even organizations that have audited their security, risk procedures and mitigation measures may find that they're not as resilient as they first thought. The bottom line for Terry and Helena: It's time again for a site security survey and updating of their risk/vulnerability matrix. With those assignments complete, they could then better prioritize and apply technologies, including security video, in a cost effective manner.

Building on What Already Exists

Many security operations already collect a myriad of data related to security incidents as well as link the data to specific security programs.

Security-related Incident Reporting, Logging

- Number of security incidents in the past 12 months
- Types of security incidents
- Primary methods used in security incidents
- Likely sources of security incidents
- Security incidents' impact on the organization
- Estimated individual and total financial losses as a result of security incidents
- Manner in which the organization learned of security incidents
- Total downtime over the past 12 months as a result of security events

Security Planning, Policies, Procedures, Technologies

- Types of decision-makers that are engaged by the organization in security issues
- Effectiveness of policies and procedures over the past year
- Elements included in the organization's security policies
- Alignment with business objectives
- Frequency of prioritizing threats by risk level
- Business issues or factors driving security spending
- Reasons used to justify security spending
- Effectiveness measures for security spending
- Confidence in security

The issue of confidence in security is essential. Depending on what comes out of the site security survey and then applied to the risk/vulnerability matrix, there may be the need – and the embedded justification – for spending on additional products and services. So the process must be based on the premise that each explored area and situation should be viewed and assessed individually, guided by the facts and matched to the business goals.

Organizations that maintain enterprise risk management programs need to engage people at all levels, from the CEO to junior staff, to learn and question.

There is no doubt that, with security demands increasing, technologies exploding and budgets ever-tightening, CSOs and security directors are becoming hard-pressed to meet security requirements.

Site Survey Adds to Right Decisions

One tool that can help is a comprehensive site survey. A survey can make it easier for Terry and Helena – and their bosses -- to see exactly what needs to be done to control access and surveillance within and outside a facility. The survey is one way to obtain answers and plan a course of action. Often, by focusing on the right actions, an enterprise can make major improvements at a cost lower than expected.

Terry decided that, at this junction, he needed to bring in a survey expert to help make the exercise both valid and believable.

A site survey is a vehicle for finding out what is right and what is wrong with a facility's perimeter and internal physical security, including electronic access control, intrusion detection and security video. Other systems such as fire alarms and sprinklers also affect these concerns. To be most effective, a site security survey should also consider the interaction of all building systems, procedures and policies.

One survey benefit is clearly identifying security gaps. Without looking at the overall picture, security can fall into the trap of short-term fixes — repairing an individual door that doesn't close properly or throwing up a camera based on increases of vandalism in a section of a parking lot. Helena rightly tells Terry that putting out these fires may not do much to improve overall security nor help with a master plan of growing security systems in the right ways.

A the first meeting with Terry and Helena, the outside site security survey consultant , suggested that a solid first step is to cover basic principles of security and the specific level of security the enterprise aims to achieve. A second step: a review of the organization’s security procedures, including access points. A discussion of access points determines whether parking lots, garages, external doors, hallways, windows and even the roof are equipped with access control and security video, where necessary.

The team decided to spotlight six elements.

1. **Description of the facility or campus.** Security and the consultant need to articulate a clear and concise understanding of the purpose of each facility and its integration to other buildings. The ability to secure a facility depends in large part on its function.

2. **Existing systems.** One major contribution a survey makes is documenting the existing systems. A comprehensive survey should note the location of every security component, such as card readers, cameras, and intrusion detection devices.

3. **Communications infrastructure.** In these days of IP-based security systems, a comprehensive site survey should document the configuration, availability and capacity of existing communications networks. Here is where Terry’s IT colleagues and system integrators play a survey role.

4. **Regulatory requirements.** In some instances, a site survey enables security to compare the existing security program against regulatory and compliance requirements.

5. **Power availability.** The access and security video camera points surveyed need power. In addition, remote locations and new locations have power needs, too.

6. **Site preparation.** The survey team also should look for conditions that may impede or preclude the effective use of an electronic security system.

With that information written down, a survey tour will be more effective, they all agreed.

So Terry, Helena and their consultant, armed with a clipboard of survey forms and digital cameras, first walked outside and around the various building perimeters to get a better understanding of how the enterprise is laid out from a security perspective. Think of it is an onion with an outer layer and layers going into the center or multiple centers with the most important assets most protected.

Comprehensive Survey with Details, Photos

They number and photograph vehicle and people entrances throughout the campus, useful in developing later recommendations or in making changes of security camera locations and their views.

The consultant had another suggestion. Grade each access and security video point: Grade A is for those functioning properly. Grade B function properly, but have cosmetic issues. Grade C is for doors and cameras that require maintenance or changes in positioning. Grade D indicates that a defective or ineffective item needs to be replaced or upgraded. Grade F indicates a need for a camera or, in the case of door controls, a code violation, which will require a new installation or product replacement.

Here is a sample of the forms in the site security survey. The first few have been filled out with example data while the others can be cut and pasted into a working survey form.

Overall building:

1. Facility address: ____800 W. Widget Blvd_____
2. Description of building: ____Mixed Use Office Building_____
3. Purpose(s) of Building: _____Sales and IT Support_____
4. Normal working hours
   - M-F Hours; personnel numbers; supervisor/manager numbers
   - Sat Hours; personnel numbers; supervisor/manager numbers
   - Sun Hours; personnel numbers; supervisor/manager numbers
   - Holidays Hours; personnel numbers; supervisor/manager numbers

Overall Access:

1. No identification _____
2. Badge _____
3. Pass _____
4. Security officer _____Yes – Regular Office Hours_
5. Receptionist _____
6. Keys _____Yes_____
7. Electronic card _____Yes_____

Overall Perimeter:

1. Is the perimeter clearly defined by a fence, wall or other type of physical barrier? _____Fence_____
2. Does the barrier limit or control vehicle or pedestrian access to the facility? Or both? _____Both_____
3. Security signage at perimeter? _____No_____
4. Electronic access controls at perimeter? _____Yes - Limited_____
5. Intrusion detection at perimeter? _____No_____
6. Security video at perimeter? _____Yes_____
7. Security officer patrols at perimeter? _____Yes Regular Hours_____

One specific survey of the parking lot, garage:

1. Total square footage _____
2. Capacity by vehicles _____
3. Number, location of vehicle entrances, exits _____
4. Levels _____
5. Elevators, staircases _____
6. Emergency telephones _____
7. Gates _____
8. Electronic card access control _____
9. Lighting – number of lights _____
10. Security video – number of cameras, location of each camera, age of cameras _____
11. Monitored video, real-time, recorded or both _____
12. Areas not covered by video _____

Overall building entrances:

1. The number, location of entrance doors _____
2. Hours of operation _____
3. Traffic through each _____
4. Intrusion detection _____
5. Electronic access controls _____
6. Keys and locks _____
7. Security video _____
8. Security officer, receptionist _____

Specific for one door -- Door Number 8:

1. Type of door _____
2. Hours of operation _____
3. Traffic through it _____
4. Intrusion detection _____
5. Electronic access control _____
6. Keys and locks _____
7. Security video
    a. Type of camera(s) _____
    b. Location of camera(s) _____
    c. View from camera(s) _____
    d. Type of monitoring _____
    e. Age of camera(s) _____
    f. Power to camera(s) _____

8. Security officer, receptionist _____

The task of reviewing all aspects of a facility and existing security technologies may seem overwhelming. But the recommendations often involve solutions with little or no cost, from cost effective ways to extend the coexistence of analog and digital to the expansion of the IP video system.

At times, a site security survey may be performed in conjunction with a planned expansion or a merger or acquisition of other facilities. This is a real opportunity to upgrade security in an entire building, and eliminates the confusion and possible security lapses that could result from conflicting security systems.

Putting Matrix Numbers to the Effort

The next step of the site security survey is appreciating the threats and vulnerabilities associated with the site, which gets Terry and Helena to their risk/vulnerability matrix.

Different than a site security survey, a threat assessment considers the full spectrum of threats (i.e., natural, man-made, accidental) for a facility, location or camera point. The assessment adds supporting information to evaluate the likelihood of occurrence for each threat. For natural threats, historical data concerning frequency of occurrence for given natural disasters such as tornadoes, hurricanes, floods, fire, or earthquakes can be used to determine the credibility of the given threat. For criminal threats, incident reports on site and the crime rates in the surrounding area provide a good indicator of the type of criminal activity that may threaten the facility.

After saying good-bye to their consultant, Terry and Helena work on threat assessments and development of their risk/vulnerability matrix. In a meeting room they posted the general threats they previously identified.

- Accidents involving employees and visitors
- Natural disasters
- Data loss
- Fraud
- Intellectual espionage
- Vandalism
- Threats to people
- Physical theft
- Brand and reputation attacks

And then they ranked the potential impact on the business for each. Impact of loss is the degree to which the mission of the business is impaired by a successful attack from the given threat. A key component of the vulnerability assessment is properly defining the ratings for impact of loss and vulnerability. Helena provided a sample set of definitions for impact of loss she found on the Web.

- **Devastating:** The facility or the enterprise's reputation is damaged or contaminated beyond near-term use or value. Most items or assets are lost, destroyed, or damaged beyond repair/restoration. A violent incident may close the facility or a crucial part of it for a significant number of days. The number of visitors to the facility and others in the organization may be reduced by up to 75 percent for a period of time.
  Example: An earthquake hits an area including a business park.
- **Severe:** The facility or the enterprise's reputation is partially damaged or contaminated. Examples include partial structure breach resulting in weather/water or a severe criminal incident, smoke, workplace violence, major fraud, or fire damage to some areas. Some items or assets in the facility are damaged beyond repair, but the facility remains mostly intact. The entire facility may be closed for a shorter period of time. The

number of visitors to the facility and others in the organization may be reduced by up to 50 percent for a limited period of time.
Example: A workplace violence incident that includes multiple loss of life and national media coverage.

- **Noticeable:** The facility is temporarily closed or unable to operate, but can continue without an interruption of more than one day. A limited number of assets may be damaged, but the majority of the facility is not affected. The number of visitors to the facility and others in the organization may be reduced by up to 25 percent for a limited period of time.
  Example: An insider disabled the server room air conditioning in revenge for a lost promotion.
- **Minor:** The facility experiences no significant impact on operations (downtime is less than four hours) and there is no loss of major assets.
  Example: A vandal writes on a parking garage wall.

Vulnerability is often a combination of the attractiveness of a facility as a target and the level of deterrence or defense provided by existing countermeasures that can include policies, procedures, products and services. Target attractiveness is a measure of the asset, reputation, or facility in the eyes of an aggressor and is influenced by the function and/or symbolic importance of the facility.

Sample definitions for vulnerability ratings are as follows:

- **Very High:** A high profile facility or a section of it that provides a very attractive target for potential adversaries, and the level of deterrence or defense provided by the existing countermeasures is inadequate.
- **High:** A high profile facility or a moderate profile facility that provides a somewhat attractive target or the level of deterrence or defense provided by the existing countermeasures is inadequate.
- **Moderate:** This is a moderate profile facility that provides a potential target or the level of deterrence or defense provided by the existing countermeasures is marginally adequate.
- **Low:** This is not a high profile or moderate profile facility and provides a possible target or the level of deterrence or defense provided by the existing countermeasures is adequate.

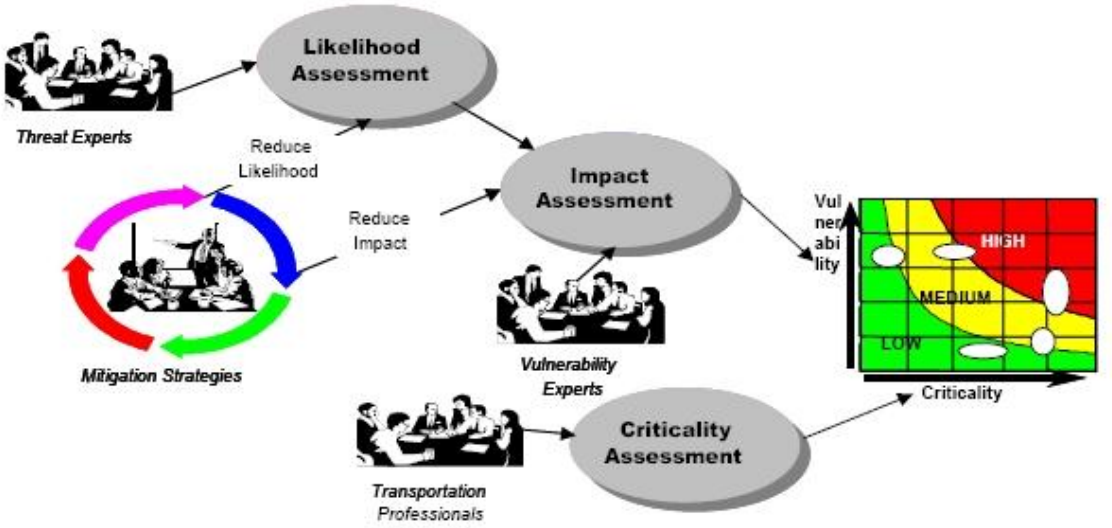
A combination of the impact of loss rating and the vulnerability rating can be used to evaluate the potential risk to the facility from a given threat.

A risk/vulnerability matrix can display overall elements or drill down to specific locations such as the perimeter, parking garage, entrance/exit doors, hallways, computer center, security command and control.

Matrix identifying levels of risk

	Vulnerability to Threat			
Impact of Loss	**Very High**	**High**	**Moderate**	**Low**
Devastating				
Severe				
Noticeable				
Minor				

	These risks are high. Countermeasures recommended to mitigate these risks should be implemented as soon as possible.
	These risks are moderate. Countermeasure implementation should be planned in the near future.
	These risks are low. Countermeasure implementation will enhance security, but is of less urgency than the above risks.



Terry then mentioned the need to fill in the matrix based on specific threats linked to specific locations and their existing security measures. Terry and Helena posted on the meeting room wall a chart (See chart on previous page.) he was given by a security colleague at a nearby transportation firm but which could be applied to any type of enterprise.

There are numerous practical outcomes of the overall exercise.

For Terry and Helena, one is the parking lot. Noting that the lot is in an urban neighborhood, that there has been escalating numbers of incidents of vandalism and trespassing, that the CEO and workers have all mentioned feeling less secure when using the lot while local law enforcement have recently requested more detailed security video of incidents, the security pair placed this area in the severe impact on loss and high vulnerability to threats on their matrix.

They then went back to the site security survey to discover – in its grading and details – that some of the current cameras covering the lot were missing some sections of it. What should we do to add more effective countermeasures, Terry asked Helena. The decision was one which plays on the coexistence strategy. Helena proposed not to add more analog cameras but to add fewer but more powerful megapixel cameras that have wider coverage and yield more details in terms of forensics. The cameras would have on-board storage and levels of intelligence so as not to tax the communications infrastructure.

Another example is the hallway leading to the firm's computer center in which beats the heart of the enterprise's computer and communications efforts. Thanks to the company's growing reliance on information services and the converting of telephones to an IP-based system, Terry increased the impact of loss to devastating and vulnerability to very high since security countermeasures have not change much.

The pair agreed to add biometrics access controls to the doors of the computer center and to better integrate security video at key doorways.

One outcome of the site security survey and risk/vulnerability matrix exercises, Terry and Helena chose to upgrade security inside and around the perimeter of the computer and communications center. They zoomed in on indoor mini domes.

Infinova's V1731N–M series vandal resistant IP mini PTZ dome is compact and light weight with an inner step motor, slip ring, rotation bearing, timing PCB board and transmission gear. The V1731N-M series IP mini PTZ dome features continuous 360° rotation, with super sensitivity, auto focus, auto iris, and backlight compensation. These cameras provide quality images under any lighting conditions. The OSD menu allows for the ease of installation and maintenance.

Infinova' s V1731N–M series vandal resistant IP mini PTZ dome deploy advanced video encoding technology, available with both MPEG-4 and MJPEG format. This unique design allows users to select the desired compression format for storage or live view based on the network bandwidth. Bi-directional audio not only enables audible sound in the surveillance field, but also over the intercom. It also features programmable motion detection and an SD card for front information storage. They can automatically record if any alarm occurs, and also support manual recording as well as automatic recording when network anomaly, which ensures the high security of your surveillance system.

For all their proposed changes, thanks to the site security survey and risk/vulnerability matrix, Terry and Helena had the data to more accurately assess their operation overall and in detail as well as use the exercise to both justify purchases to their boss and fit the new technology into the legacy systems in a cost-effective way.

What's Coming up Next

In the next in this series of Infinova white papers, there will be a step by step review of security lighting, its ability to fight crime and mitigate incidents when properly chosen and installed and how it complements the effective use of security video to provide usable evidence.

By helping channel partners provide their customers with complete, affordable, best-in-class, large and small video surveillance solutions, Infinova helps integrators generate more business more profitably. Leveraging a manufacturing process certified to ISO 9001:2008 standards and over 250 engineers with a list of video industry firsts, Infinova channel partners provide their end-users with industry-acknowledged product reliability and technical leadership.

So that Infinova channel partners can create complete solutions, Infinova provides IP surveillance cameras and components, CCTV analog cameras, DVRs and components, camera accessories, monitors, power supplies and fiber optics communications devices. Infinova also has the technical ability and manufacturing flexibility to let integrators propose customized solutions. In addition, Infinova will partner with other manufacturers making other surveillance equipment and software to help its channel partners create turnkey solutions. Contrary to most other companies, Infinova will back-up their partners' products as well as its own to assure both the integrator and its customers that one call – to Infinova only – takes care of everything.

Infinova works diligently to assure its channel partners can provide cost-conscious solutions. With Infinova's hybrid systems, channel partners can propose systems that protect a customer's investment in its already-installed analog surveillance system but that also put them on a dynamic migration pathway to IP systems.

Infinova is lauded for its exceptional maintenance programs. A major highlight is the company's 24-hour advanced replacement policy in which a substitute product is shipped immediately upon notice of a problem.

With such customer focus, Infinova is often referred to as "the integrators' manufacturer."

Global Contact Information

Infinova®
The Integrator's Manufacturer

United States
Infinova
51 Stouts Lane
Monmouth Junction, NJ, 08852
United States
Phone: +1 732-355-9100
+1 888-685-2002 (toll-free)
Fax: +1 732-355-9101
Email: Sales@infinova.com

Latin America
Miami: +1-954-990-0787
Mexico: +52-55-5392-1735
Venezuela: +58-212-336-0661
Brazil: +55-11-7479-5640
Email: Sales-LAR@infinova.com

Europe
Phone: +40 2 6841 5582
Email: Sales-EUR@infinova.com

Middle East
Phone: +965 247 5678
Email: Sales-ME@infinova.com

India
Sales: +0091 9980728579
(South and East India)
Email: Sales-IND@infinova.com

Hong Kong
Phone: +852 2795 6540
Email: Sales-HK@infinova.com