Conducting Virtual Security Assessments

By: Ilya Umanskiy

FOR SENIOR DECISION MAKERS:

In a world with countries in and out of pandemic lockdowns and a 70% decline in international travel (projected by the end of 2020 according to the UN World Travel Organization), the word "virtual" is hardly new. We are adapting to the use of virtual tools out of necessity, to help keep our personal and professional lives moving forward.

Like all of us individually, as well as public and private organizations worldwide are now at different stages of adaptation to the new reality. One constant in all of this is risk management as a way to assure operational resilience.

No organization has completely abandoned business objectives or the need to produce results for their customers and stakeholders. In fact, organizations increased their search for and implementation of innovative strategies and processes. Just notice how popular the phrase "digital transformation" has become.

The field of security (asset protection) has embraced innovation as well. Look at the recent wave of contactless and environment monitoring technologies hitting the market.

I would like to share with you my experience around innovating in security, to help organizations achieve and maintain their resilience during these trying times.

While a remote assessment of an environment - relative to its security is not new - the tools available to security practitioners today have made it a viable option for helping organizations get the same or better understanding of their threats, vulnerabilities, and risks - relative to assets and objectives when compared with results of a traditional on-site security assessment. This option is also very attractive because it achieves the same, or better, results while eliminating travel costs and increasing overall efficiency of each assessment.

Aside from cost savings and increased efficiency, there are a few additional benefits virtual security assessments can deliver.

Image Credit: Freepik.com

INCREASED COLLABORATION

It may sound strange, but a virtual assessment creates an opportunity for security assessors to more closely engage with local teams. This is a natural development since local knowledge and guidance is what ultimately helps such assessments to be completed successfully. Through experience, I noticed that coordination and communication with the local team during an assessment becomes more positive and consistent. Local representatives ask more questions and actively engage in knowledge sharing.

On multiple occasions local team representatives shared that they wanted to increase their own competence in security so that they could help manage protection day-to-day, instead of relying on help from people who are less familiar with their facility. In this way, security assessors are treated as advisors on an ongoing basis to help with less routine and more complicated security matters.

BETTER KNOWLEDGE TRANSFER

It may be simply due to the collaborative nature of a virtual assessment and the natural need for security assessors to rely more heavily on the local team, but knowledge transfer becomes a necessity. I have found myself in a teaching and coaching role more often during

virtual assessments – helping local team members understand various protection concepts and apply them on an ongoing basis. For example, on several occasions I have coached local teams to look for nuances in security guard performance, operation of access control and video surveillance systems, and selection of quality products and competent contractors.

ENABLING YOUR TEAM

To help build your capability in virtual security assessments, I offer you a simple, step-by-step methodology.

Image Credit: Freepik.com

Step 1 - Facility Type

Security of any facility, of any size, and of any type can be assessed virtually. You need to have a clear understanding of the facility's surrounding area and property boundary, exterior grounds, and functional compartmentalization of buildings. All this information can be obtained by reviewing available mapping data, architectural site and building drawings, as well as photographs and video footage provided by local representatives. In some cases, use of drones can also be very helpful, but will add to the cost of the assessment.

Step 2 – Scoping

Please don't be surprised by this sequence of steps. Knowledge of the facility's type and general information about it is very necessary for finalizing the scope of your virtual security assessment. Having this information in advance will help you determine several critical elements of upcoming work such as:

- **Time required to complete the assessment.** This will be based on the facility's size and complexity relative to functions, critical assets, and availability of local support.
- **What needs to be assessed?** Often, security assessments may be performed for certain portions of facilities or certain assets. Having this established up-front will help focus your efforts and determine what tools and local support you may need to conduct your virtual assessment.
- **What local support is required?** Although the assessment is virtual, local responsible management and stakeholders should be identified at this stage to ensure operational support and availability for interviews. In most cases, you will need to engage with leaders of every function at the local facility.

Step 3 – Local Contact

As noted above, engagement with local responsible management and stakeholders will help you collect most of the necessary information for your assessment. A local representative with extensive knowledge of the facility and its operations will serve as your "eyes and ears", providing photos / videos of existing conditions, as well as answers to most questions.

Step 4 – Information Gathering

In any assessment – virtual or on-site – practitioners collect high volumes of information in different formats and on different pertinent topics: through interviews, observations, and shared documentation. It is important to organize all information into familiar categories to make your collection and analysis as efficient as possible. Here's a suggested outline:

- General property profile (example: address, setting, primary functions, number of people, size, number of buildings, pedestrian and vehicle access, adjacent facilities, profile of a larger 3–5-kilometer radius, etc.)
- People interviewed and results of individual / group interviews
- Key operational objectives of the facility
- Mission-critical assets (prioritized by criticality relative to impact on operations, financial resources, and reputation)
- Past incident history
- Known threats against mission-critical assets and perceived probability of their occurrence
- Current protection measures (operational, technological, physical, and incident management controls)
- Current documentation related to protection measures (policies, procedures, plans, guidelines, workflows, etc.)
- Who at the site is currently responsible for protection of assets and what is their level of competence and capability?
- Known vulnerabilities

Step 5 – Analysis

An obvious progression from information gathering is the analysis. The most important objective is to confirm vulnerability of mission-critical assets to known threats and relate this to probability of threat occurrence, as well as the impact on operations, reputation, and financial health.

This can be done qualitatively and quantitatively. The best way of expressing the loss impact is typically in financial terms (example: loss of asset X will cost the organization N dollars) to help senior decision makers clearly understand your findings and recommendations.

Once this is achieved, a set of actionable recommendations should be developed – emphasis on the word "actionable".

Step 6 – Reporting

This is one of the most challenging aspects in any virtual assessment because the quality and acceptance of re-

porting will predict the extent of improvement in security and future consistency of protection measures. Please consider the following key points:

1. Reporting should be delivered verbally - as a briefing on the main findings and recommendations – and as in writing, with a focus on ease of understanding and implementation of improvements.
2. It is useful to highlight what works well and, importantly, praise the local team for their efforts before moving on to exposures and recommended mitigations.
3. The more your own reporting helps to enable the local team, the better and more consistent the outcome will be. So, please think about addressing local capabilities, simple process and technology changes, as well as carefully designed continuous training.

Step 7 – Follow-up

This is an opportunity for security assessors to solidify their relationships with local site representatives and decision makers. Through carefully structured and delivered follow-up, a security assessor can help guide the local team, monitor improvement progress, celebrate accomplishments, and take note of any persistent challenges.

The focus here is on being a helpful guide and building a strong, collaborative relationship, because any assessment – virtual or in-person – will typically need to be repeated with the assistance of the local team.

USEFUL TOOLS AND STRATEGIES

As you contemplate future virtual security assessments, here are a few tools and strategies to consider:

1. Google Maps / Google Earth provide very good satellite and street view access for assessing site conditions as well as the surrounding environment in many locations around the world. The point-to-point distance measurement tool can be accessed by right-clicking on any zone of the map.
2. Open-source threat information can often be obtained from the following:
    a. United Nations Office on Drugs and Crime (unodc.org) publishes an annual report on crime trends and provides visualizations based on geography and crime types
    b. Local law enforcement organizations may be helpful with information regarding local crime trends
    c. Interpol publishes an annual report on crime trends and many other useful analyses (https://www.interpol.int/en/Resources/Documents)
3. Adobe Acrobat Reader and AutoDesk Design Review file viewers can be very useful for working with site architectural and other technical plans.
4. Microsoft PowerPoint or iOS Keynote can be used for arranging and annotating facility photos and any other graphics for presenting during reporting and follow-up.

Image Credit: Freepik.com

5. Agreeing on and following a labeling and filing scheme for all project documents will save time during information collection, analysis, reporting, and follow-up.
6. Starting each interview with an offer to answer any questions and then sharing what you already know about the facility will help save time and build rapport with local team members.
7. Structuring assessment reports, with a focus on easy navigation and presentation of the most important details in the executive summary, will help increase mutual understanding and further collaboration. Use of color-coding and graphics is encouraged. A simple guide can be found here: https://www.interaction-design.org/literature/article/ux-report-writing

8. Conclusion

Leading during uncertain times is challenging, to say the least.

The objective of this article is to help senior decision makers solve challenges of protecting their business operations in different places, without additional logistical and financial burdens, while improving collaboration and knowledge transfer. This is how we all can achieve resilience in practice.

Stay safe and well.

Ilya Umanskiy GRCP, RAMCAP, MA

From Moscow, to New York, to Hong Kong, and most places in between – Ilya has been there, in boardrooms and in the field, building his vast experience. His dedicated work has touched a wide spectrum of risk mitigation and resilience operations, including threat and vulnerability assessments, risk management framework development, design and implementation of technological, physical, and operational asset protection controls, and third-party due diligence, to name a few.