CORPORATE SITUATIONAL AWARENESS: **WATCH YOUR FRONT!**

JUNE 2018

SWAN ISLAND NETWORKS

SUMMARY

Your organization faces multiple risks every day, from a disgruntled ex-employee planning revenge to a Pacific cyclone delaying vital supply chain shipments, and a host of threats in between. An isolated issue can become world news and brand-destroying in minutes. A major issue can devastate your organization, causing the loss of life, property, reputation, and continuity. Without a strong set of situational awareness tools and policies, you face a tsunami of disjointed information that can cause you to miss important indicators and mismanage your response. It's vital to be informed, aware, and prepared for anything. What you don't know ***can*** hurt you.

In this paper, we'll look at multiple aspects of situational awareness in organizations. We've broken the information into sections for easier reading and consumption. If you're interested in a follow up discussion or have critical feedback, we'd welcome either.

SECTIONS

WHAT IS SITUATIONAL AWARENESS?

Perception, comprehension, and projection are three of the core definitional terms of situational awareness. These could be understood as identifying threats, understanding their importance and potential impact, and strategizing different possible responses. Situational awareness is, at its core, having an accurate understanding of your surroundings: where you are, what could happen, and recognizing problem indicators before an incident. Once a threat manifests, knowing what happened, what is happening now, where critical resources stand, and what is changing all become part of an intense effort to understand and communicate with response efforts. Paying attention to the risks, threats, contingencies, and response capability available to you is key and should start with a proactive effort.

"DO NOT SPARE ANY REASONABLE EXPENSE TO COME AT EARLY AND TRUE INFORMATION..."

George Washington, the commanding general of the Continental Army and later first president of the United States understood the importance of analyzing the situation around him, and how to utilize his resources in the most effective way. He spent over 10% of his limited resources on intelligence, spy craft, and troop movements. It paid off well in his historic victory over much stronger forces.

Some wide-ranging examples where lack of situational awareness can have or had devastating consequences:

Texting while driving: Those few seconds it takes to look at the screen and pound out a message can cause you to lose awareness of the road and the car that just braked in front of you, or where the lines are. Losing situational awareness can kill and maim in an instant.

2004 Asian Tsunami: Many people knew there was a gigantic wave heading for many different parts of the Pacific Ocean right after the entire planet shook from the major earthquake. Warning systems for the 14 countries, and especially the rural communities impacted, were not in place and somewhere between 240,000 and 280,000 casualties resulted.

Parkland shootings: Many people saw the signs of an imminent disaster around Nikolas Cruz and spoke up about it, but these warnings went unpursued. The result was the loss of innocent lives.

EXAMPLES WHERE SITUATIONAL AWARENESS AND REAL-TIME ADJUSTMENT MADE A MAJOR DIFFERENCE IN RESPONSE, MITIGATING THE IMPACT ON LIVES, PROPERTY, OR CONTINUITY:

US Airways 1549: When this flight took off from LaGuardia in New York City heading for Seattle, all looked normal and clear for an uneventful flight. Immediately upon takeoff, however, the plane encountered a flock of birds and both engines were suddenly without power. Captain "Sully" Sullenberger was aware of his options and prepared; he was able to land the plane on the Hudson River and avoid any loss of life.

Hurricane/fire evacuations: With far better situational awareness today, countless lives have been saved by proactively ordering evacuations of coastal areas prior to a storm's arrival, or areas likely to be impacted by rapidly spreading forest fires. Detection, monitoring, response, and better warning systems integrated together help give many more people the situational awareness they need for vital decision making.

Automatic braking systems: High-end automobiles are being equipped with proactive braking systems designed to minimize rear-end collisions. The vehicle's computer monitors the distance and speed between vehicles, and can invoke emergency braking when needed.

9/11 Hero – Rick Rescorla: After the 1993 bombing of the World Trade Center, Rick Rescorla, the executive in charge of security at Morgan Stanley's WTC offices wanted to move and find new space; he was sure that the current building would undergo another attack. When that request was denied, he prepared and practiced an evacuation plan for all the Morgan Stanley employees. When 9/11 happened, Rick's preparedness plan and execution on that critical day was credited with saving over 2,600 lives. He gave his life going back into the falling tower to try to save others, but saved all those he was responsible for.

WHAT ARE SOME BEST PRACTICES FOR BUILDING AND EXPANDING ON SITUATIONAL AWARENESS CAPABILITY?

LONG-TERM AWARENESS

Pervasive threat (years/decades):

- The Big One: earthquakes in Los Angeles, San Francisco, and the Pacific Northwest, globally. We know the tectonic plates are going to shift; we also know that we have infrastructure that will be severely tested. History shows us that cascading failures produce a wide variety of unanticipated problems.
- Climate change impacts: Sea level rise, storm surge implications – Houston has had three 500 year flood events in three years. Superstorm Sandy brought a very large storm surge to the New York City region. What could impact your facilities as time progresses? This category of events can be easy to discount, resulting in avoiding or minimizing preparedness efforts. A false sense of security can be deadly.

EMERGING THREATS

Months to get ready:

- Zika virus and other pandemics: Health threats merge continually. Do you have them on your organization's radar?
- Hurricane season: If your organization is in the impact zone, having multiple contingency plans for the overall approach to storms will augment your efforts when one shows up.
- Shared efforts for monitoring and preparation are feasible with these types of threats. Does your organization have good relationships with other organizations who can work with you?
- Preparedness and urgency are critical. The 1918 Spanish Flu, which killed up to 50 million people, would take 11-18 days versus 18 months to move around the planet with today's transportation systems and far higher population.

SHORT TERM AWARENESS / RESPONSE CYCLE

Rapidly developing situations that threaten lives, property, reputation, or continuity:

- Hurricane identified to hit in five days: Shifting of crucial resources, extra generator fuel, minimal vacations for response staff.
- Urban area disruption due to large scale protests: Employee notification, additional monitoring, (e.g. video and social), and alternative transportation planning.
- Focused preparation, mitigation, response, and recovery cycle should all be scripted.

"NO NOTICE" DISASTER

Real-time reactions needed:

- Terrorist or insider attack (physical or cyber).
- Pipeline failure or oil tanker crash.
- Situational awareness tools can help during response/recovery by aggregating multiple information sources in near real time: cameras, news sources, field reports, partner information, status updates, and more.

WHERE DOES MY ORGANIZATION GET INTELLIGENCE FOR QUALITY SITUATIONAL AWARENESS?

OPEN SOURCE NEWS INFORMATION

There are thousands of sources on the web, television, radio, and other media. The web is fast, updated continually, and makes information gathering easier. Critical video clips will also be posted in minutes or seconds.

SOCIAL MEDIA - RAW

Raw social media can provide some of the earliest indications of a event and is open to the entire world, so sharing issues are minimized. Social media can also be wrong, so it's important to verify and correlate.

SOCIAL MEDIA – OFFICIAL FEEDS

Many municipalities have at least one social media feed, typically Twitter, that can be used as a validated source.

PARTNERS AND CONTRACTORS

You can create methods for your external connections to send you information that can be incorporated into your awareness picture.

GOVERNMENT OFFICIAL SOURCES

Severe weather, earthquakes, and other events are quickly made available to web-based sources. Earthquake tracking by USGS is particularly impressive; the alerts contain geolocation and magnitude information that can be quickly displayed on a map.

FUTURE EVENT SITES

Upcoming protests and other large events such as marathons and parades can have a big impact on traffic, security, and other areas. Knowing when and where they are occurring can provide valuable awareness to your organization.

INTERNAL PERSONNEL

Internal personnel are invaluable for information. Have a clear "See Something, Say Something" policy, and train staff how to report information via multiple channels, such as email, text, phone, apps, etc.

INTERNAL SECURITY SYSTEMS

Your internal systems for alarms, video monitoring, identification, and many others can be integrated to alert your central situational awareness system.

JUSTIFICATION & ASSESSMENT

UNDERSTANDING YOUR APPETITE FOR RISK

Your organization needs to understand how important it is to manage risk and weigh the costs of risk management against the potential impacts. This is very different if you are a retail chain with three local locations or a pharmaceutical company with world-wide manufacturing and distribution points.

SCOPING YOUR VULNERABILITIES

Doing a strong assessment of the types of threats you are likely to encounter will help organize your efforts. This is usually an internal and external effort, combining outside consulting with internal risk management, security, and business continuity personnel.

ASSIGNING ACCOUNTABILITY WITHIN THE ORGANIZATION

There are multiple layers of accountability to be considered, with strategic and tactical being the ones that most organizations focus on. The Board, C-Suite, and Chief Risk Officer take a broad look at risk, and establish the direction and budget for the tactical response groups inside the organization.

EVALUATING RETURN ON INVESTMENT (ROI) ELEMENTS

Preparedness incurs short-term and long-term costs. Make sure your finance team understands the long-term savings of risk reduction, and is aware of the impact that preparedness, monitoring, and response will have on the bottom line.

- **Loss of life and/or property:** This impact on an organization can be devastating in many different ways, and many organizations consider safety of its people a core justification for a strong preparedness program.
- **Long term recovery disruptions costs:** Many organizations have elements in their operations that, if disabled, will have months or even years of impact. A single point of failure, rendered inoperable, will cause cascading effects.
- **Brand impact costs:** With the speed and viral effect of social media, events that impact your brand (both good and bad) can go from unknown to global awareness in hours. This is a critical area for pre-planning, monitoring, and rapid response.
- **Time savings from redundant/crossover efforts:** When you perform an assessment of your organization, you may be surprised to realize how much redundant effort is being spent on gathering situational awareness, and how data is not being shared. Having a strong, well-managed program can channel these efforts into an information stream that can be leveraged across the organization.

WHAT ARE SOME BEST PRACTICES FOR BUILDING AND EXPANDING A SITUATIONAL AWARENESS CAPABILITY?

DESIGN · DEVELOPMENT · DEPLOYMENT

This section could easily be a book unto itself, but we've covered a few of the key points you need to consider. There are multiple providers who can help your organization build a comprehensive strategy, choose tools and partners, and begin the process of building a capable program.

IDENTIFICATION OF STRATEGIC AND TACTICAL RESPONSIBILITY

Assigning the right people in the organization as central points of accountability is key. This function has to be strategic to interface with the Board and C-Suite, and tactical to handle group response programs.

GAP ANALYSIS

Finding the areas where your organization is strong and the areas where you need improvement will help prioritize your efforts and allocations.

FUTURE ASSESSMENT

This is a long-term effort, so understanding what could – and what will – change over the next three to seven years is another important element in your planning and capability deployment process. For example, investing in a fixed-location non-intelligent video system may be a poor idea, given the rapid changes around intelligent video and drones/robots.

PARTNERS

Having the right partners can give your situational awareness and response programs added flexibility and surge capabilities. Depending on your situation, partners can provide a wide array of options, such as outsourcing your Security Operations Center (SOC), providing multiple integrated technology systems and/or external feeds of critical information.

SOFTWARE TOOLS AND SYSTEMS

Picking the software that will best support your effort is crucial, and the training and integration efforts are equally important. These software capabilities will touch many parts of the organization, so ease of use and interoperability with existing systems should be given extra weight in the decision-making process.

COMMON MISTAKES AROUND ENTERPRISE SITUATIONAL AWARENESS

MISTAKE 1. WE WON'T DRIVE FROM THE BOARD/C-SUITE LEVEL

Boards of Directors and C-Suite execs are accountable for all aspects of the organization's operation and survival. It is key that the strategies for situational awareness and response line up with corporate priorities.

MISTAKE 2. WE'LL ALL WATCH THE INTERNET

If everyone is responsible, then nobody is responsible. If everyone is trying to watch for threats, there is a huge amount of redundant effort that is being wasted every day.

MISTAKE 3. WE'LL MONITOR ONLY DURING THE BUSINESS DAY

Bad things happen after hours, and for large companies, the sun may never set across your geographic footprint. You need to have a method for monitoring and notification of critical events 24 by 7.

MISTAKE 4. WE'LL RELY ON A SINGLE NEWS SOURCE

CNN is a great worldwide news channel, but will not give you all the specifics that you need. If there is a highway shutdown that will block all your employees getting to work, or a broken water pipe inside your facility, you need to consider more sources of threat intelligence.

MISTAKE 5. WE'LL COMMUNICATE POORLY

Organizations need to a bullet-proof means of alerting and notifying the right people in an emergency. This is much easier than 25 years ago, with our always-on cell phone culture, but still fraught with issues if key people are on vacation or compromised by the incident at hand.

HOW DOES SITUATIONAL AWARENESS INTEGRATE WITH OTHER SECURITY SYSTEMS?

SITUATIONAL AWARENESS CAN DRIVE PROACTIVE PREPAREDNESS

When an organization considers the multitude of threats it could encounter, it's a natural process to start developing the downstream response scenarios. Part of that effort is looking at how the various functions and tools can work together, both during an incident and as a means to prevent or mitigate emerging problems.

YOUR OTHER SYSTEMS CAN FEED INTO:

ALARM AND VIDEO MONITORING

Internal systems can send exception alerts to your situational awareness tool. Imagine that you get an alert that a license plate belonging to a recently fired, threatening employee has just entered your corporate parking lot; this type of alert would give you far more reaction time.

MOBILE PHONE APPS

All of your employees and partners can provide real-time situational awareness reports using their mobile phones and basic communications applications – when you see something, say something efforts can be linked into central situational awareness efforts.

EMAIL

Desktop email can be another great way of leveraging everyone into helping with situational awareness. Situational awareness systems can have a direct email integration capability that allows information from many places to be consolidated into a stronger, central picture.

SITUATIONAL AWARENESS CAN FEED INFORMATION TO RESPONSE SYSTEMS

Situational awareness should go into overdrive during an incident, continuing to gather highly specific information that can be utilized by responders during an incident.

INCIDENT RESPONSE

The latest information is critical when responding to an incident, and situational awareness solutions can help provide that information to decisions being made in real time. There may be a choice that is dependent on the flow of two major rivers, or a directional change of a major ground fire.

MASS NOTIFICATION

Situational awareness can provide information that may be repurposed to send to everyone in the organization, or highly targeted groups that are dealing with a particular incident.

CRISIS COMMUNICATIONS

Crisis communications systems allow distributed groups to respond to an incident with centralized coordination. Situational awareness can provide external and collated information that can be folded into these response cycles.

EMERGING CAPABILITIES AND TRENDS

FLEXIBLE RESOURCES TO AUGMENT MAJOR ISSUES

Because of technological advances, distributed resources can preempt the traditional adage, “all disasters are local”. Your security operations center (SOC) can be augmented by people far from the event, giving you greater control and lower response costs.

SENSOR-BASED ALERTING FROM TODAY’S SECURITY SYSTEMS AND TOMORROW’S INTERNET OF THINGS

If you have seen the new cars with automatic collision avoidance, you get a sense of where the man/machine interface is going – technology can help with response time. Innovations with this capability are being developed and deployed in many different areas.

BLENDING OF INTERNAL AND EXTERNAL INFORMATION

Combining outside social media and news with internal mobile phone alerts, email, and internal security systems can provide a greatly enhanced composite view of the general situation or a specific incident, giving both context and scale to understanding.

COLLABORATION WITHIN INDUSTRIES OR GEOGRAPHIC REGIONS

Organizations are realizing that security and protection are vital, but that it is very expensive to do everything yourself where sharing and cooperation will enhance response and cut overall costs.

CELL PHONES

Your cell phone is getting more capable every year, and has potential to help track you in an emergency, provide you with procedures if you lose connectivity, and facilitate a two-way messaging structure for multiple incident types. Between video and still shots, cameras provide a tremendous amount of information every day.

DRONES AS INFORMATION GATHERING DEVICES

Drones are still emerging, and there is a substantial amount of policy work to be done before they become a pervasive tool. However, this technology is advancing very quickly, and is well worth the time to monitor new developments.

CONCLUSIONS

Situational awareness can be vital to your organization, providing information from a wide range of sources that can be analyzed to determine how to react to upcoming incidents, threats, and other events. Having accurate information is the first step to a long journey of understanding, analyzing, developing, and deploying these capabilities to become a part of the fabric of your organization's day to day security initiatives.

CHOOSE A FLEXIBLE, RESILIENT, HIGH-CAPACITY SOLUTION

We invite you to take a closer look at how Swan Island's TX360® can help you protect what matters through intelligence data, intelligently applied.

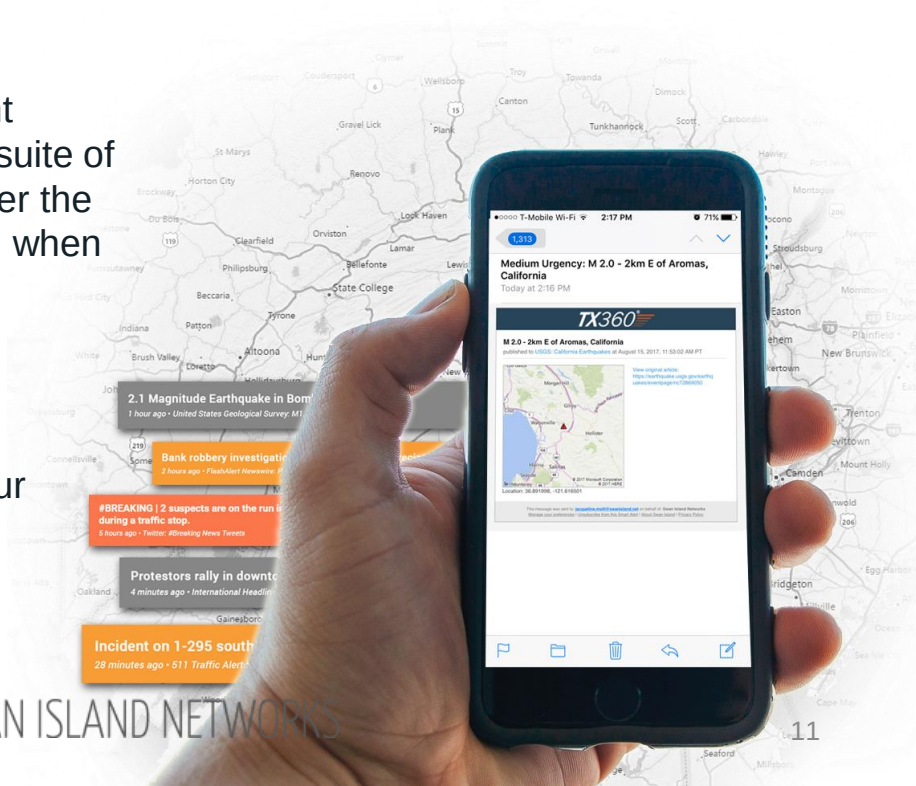
TX360®

"Distilling the flood of information into **actionable intelligence.**"

TX360 is an all-hazards threat monitoring and situational awareness service that enables highly secure and targeted delivery of critical information to security professionals and corporate leaders.

Identify and manage the most relevant emerging risks and threats with a full suite of intelligence management tools. Deliver the precise information your people need, when they need it, using Smart Alerts.

TX360 is a highly scalable and robust platform, operating on the Microsoft Azure cloud. Read on to learn how our software can help your enterprise identify threats and respond to them more effectively.



TX360®

PRODUCT FEATURES

INTELLIGENCE CHANNELS

Gather late-breaking intel from an expansive gallery of highly filtered, trusted sources, and import and curate your own feeds.

SMART ALERTS

Deliver relevant alerts to individuals and teams, tailored to each recipient's geography, authorization, preferences, and profile.

DASHBOARDS

Monitor relevant threats in real time on a common operating picture dashboard and determine the potential impact of an incident on your assets.

ASSETS

Import corporate assets and facilities locations for proximity-based threat monitoring and Smart Alerting.

- **Social media monitoring** enables access to crowd-sourced intelligence from Twitter, Flickr, YouTube, Reddit, and more.
- **Mapping capabilities** include Assets and Overlays (KML, XML, various geotagged data types), as well as traffic, cameras, and search.
- **Premium Channels** available, which leverage selectively curated feeds around a variety of topics and geographies.

PUBLIC / OPEN SOURCE FILES AND LAYERS INCLUDE:

- Severe weather (NOAA, NHC, JTWC, etc.)
- Natural disasters (USGS)
- Official city feeds/alerts (emergency, utility, roads)
- Public health
- Travel alerts
- Crime, 511, 911 as available.

SWAN ISLAND NETWORKS

Swan Island Networks has been a leader and innovator in situational intelligence and Smart Alerting for over a decade. Swan Island's TX360® platform helps you make faster, better informed decisions with highly relevant real-time alerts and a comprehensive common operating picture.

Founded in 2002 by 20-year veterans of the software and security industry, Swan Island Networks began as a software engineering lab working with the US government, focusing on R&D programs. The company has participated in a dozen contracts with government agencies such as the Department of Defense, Homeland Security, and various intelligence organizations.

TX360 is the core technology platform for the New York City Metropolitan Resilience Network (MRN), providing a common operating picture and intelligence service to hundreds of multi-national corporations. TX360 is used and resold by major security firms under a white label agreement, and is available for direct subscription through Swan Island Networks. The technology can be localized to multiple languages, is easy to use, and very affordable under a Software as a Service (SaaS) arrangement.

For more information, contact us at 503.796.7926, email info@swanisland.net or visit swanislandnetworks.com.

HEADQUARTERS

6420 SW Macadam Ave.
Suite 204
Portland, OR 97239
503.796.7926
swanislandnetworks.com

PETE O'DELL

CEO & Founder
pete.odell@swanisland.net