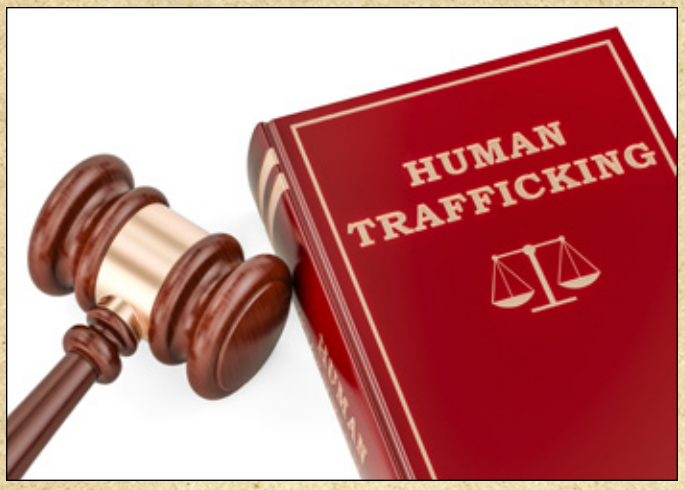
domestic preparedness .com

DomPrep Journal

Subscribe

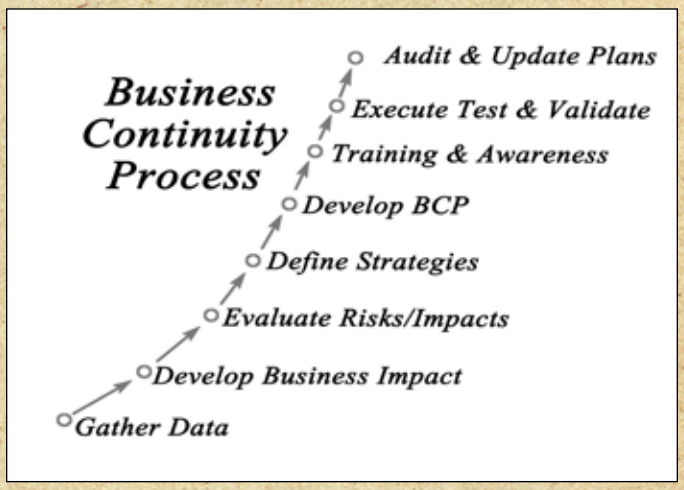
Volume 14, Issue 7, July 2018



Human Trafficking – A National Security Issue
By Richard Schoeberl & Benjamin Nivens

The Big Data Bind
By Daniel M. Gerstein

Three Ways AI Helps Prepare for Future Attacks
By Michael Ellenbogen



2018 Business Resilience Conference, Las Vegas, NV
By Rodger (Kevin) Clark

Also inside...

Podcast – Public Health Preparedness: Segment 2

Invisible Threats Exposed

AP4C

Portable Chemical Detection System
Protects First Responders, Military & Infrastructure

- Fast, Reliable Analysis of Invisible Hazards Saves Time & Lives
- Unlimited Simultaneous Detection Exposes Unknown Agents
- Low Maintenance & Operation Costs Save Money
- Rugged Handheld Design is Easy-To-Use With Minimal Training
- Complete System Includes Accessories & Case for Easy Transport

Learn More Online

PROENGIN

Chemical and Biological Detection Systems

Business Office
P.O. Box 810
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

Catherine Feinman
Editor-in-Chief
cfeinman@domprep.com

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

BioFire Defense

FLIR Systems Inc.

PROENGIN Inc.

DomPrep Journal is electronically delivered by the IMR Group Inc., P.O. Box 810, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomPrep.com

Articles are written by professional practitioners in homeland security, domestic preparedness, and related fields. Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher. Text is the opinion of the author; publisher holds no liability for their use or interpretation.

Featured in This Issue

Pictured on the Cover: (top row) Schoeberl & Bivens, Source: ©iStock.com/AlexLMX; Gerstein, Source: ©iStock.com/sinemaslow; (second row) Ellenbogen, Source: ©iStock.com/monsitj; Clark, Source: ©iStock.com/vaeenma

Our commitment to BioDefense

has allowed us to be ready

for the Ebola outbreak

in West Africa.

Now, with the FilmArray system

and our reliable BioThreat Panel,

we are able to test for 16

of the worlds deadly

biothreat pathogens

all in an hour.

Now That's Innovation!

BIOFIRE®

DEFENSE

Learn more at www.BioFireDefense.com

Securing Communities as National Security Threats Evolve

By Catherine L. Feinman

There is no quick fix for addressing all national security threats. Even if there were, it would still be challenging to keep up with the threat environment as it continually evolves at what seems to be exponential rates. The natural and manmade disasters of yesteryear are compounded with emerging cyber, technological, and other threats that once were only in the imagination of science fiction writers.

Unfortunately, the technologies that provide solutions to modern issues and needs are sometimes used to facilitate nefarious actions. For example, "big data" provide vast amounts of information that is critical for research, networking, and security, yet such data could also infringe on personal information, privacy, and security. Such technology develops quickly, with unintended consequences easily following.

Artificial intelligence is another technology that has various uses. Traditional threat detection devices like metal detectors have limited effectiveness in detecting modern non-metallic threats. However, security in today's world requires a proactive and mitigative approach. Simply reacting when an incident occurs may be too late to prevent devastating consequences.

Of course, there is always a place for human intelligence in a national security strategy. Situational awareness and recognition of warning signs can help deter crime and save lives. Human trafficking and public health threats are just two examples where human intelligence is a key component to successful mitigation. To secure communities and prepare for potential threats, a combination of emerging technologies, artificial intelligence, and human intelligence are needed.

This issue explores these national security issues and provides ways in which preparedness professionals in the public and private sectors can secure their communities and build resilience.

Human Trafficking – A National Security Issue

By Richard Schoeberl & Benjamin Nivens

The United States abolished slavery nearly 150 years ago. However, human exploitation through sex and forced labor remains a growing human rights violation and national security issue. Human trafficking is not prejudicial to nationality, age, gender, or socioeconomic status and is closer to home than most would like to consider. The exploitation and violation of human rights knows no boundaries and requires preparedness and response efforts from every country, every state, and every city.

Human trafficking is an epidemic that, according to Polaris, has affected some 40 million people globally. In the United States, it is happening to both U.S. citizens and non-U.S. citizens at equal rates – and victims are getting younger. According to the State Department's Trafficking in Persons report, 76% of trafficking victims are female – with underage females comprising 17% of that total figure. The National Runaway Switchboard estimated that 1.6 to 2.8 million runaway teens are in the United States – females representing 55%. In 2016, approximately one in six of these runaways were likely human trafficking victims according to a report issued by the National Center of Missing and Exploited Children.

Big Business & Growing Numbers

Human trafficking and human smuggling are not interchangeable:

- Human smuggling is the movement of a person across a border.
- Human trafficking is the exploitation of that person through means of force, fraud, coercion, or violence.

This national/transnational crime is rapidly subjecting victims into forced labor, sexual exploitation, debt bondage, sexual slavery, organ harvesting, and much more. Although human trafficking is illegal, it continues to be problematic and under-identified.

Polaris indicates that a record 8,759 human trafficking helpline cases were received in 2017 with an increase in percentage of hotline cases increasing 13% from 2016. There has been an 850% increase in hotline calls since its inception over the last decade that Polaris has operated the National Human Trafficking Hotline – with Florida, California, Ohio, and Texas having the highest number of reported cases in recent years.

The U.S. State Department and the International Labor Organization estimate that human trafficking is a $150 billion-a-year global business. According to the Harvard Law Review, it is quickly exceeding other high-profit crimes such as narcotics and firearms. Before 2000,

laws in the United States were simply inadequate to deal with human trafficking. Protecting and assisting victims with aftercare programs – rescue, reform, and restore – were equally inadequate. Despite legislation to combat trafficking evolving since 2000, human trafficking remains a persistent problem, the inconsistent enforcement of anti-trafficking measures raise concern, and public services for rehabilitation are still lacking. More is needed to address not only the enforcement of human trafficking laws, but the preventative and rehabilitative component of those subjected to modern-day slavery.

International Response Efforts

Despite trafficking expansion over the past century, it was not until 2000 that the first agreement (the United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children) was drafted recognizing modern-day slavery and expanding the characterization to consist of forced labor migration and organ harvesting. Responding to the trafficking increase, the U.S. Congress ratified the Victims of Trafficking and Violence Protection Act (TVPA) in 2000. Regardless, the effectiveness of laws enacted to combat trafficking today is unknown mainly because the crime goes unidentified or is prosecuted or minimized under other laws such prostitution. The TVPA addresses human trafficking crimes and enhances the existing crimes of peonage, involuntary servitude, and slavery. TVPA additionally protects victims and helps re-establish their lives through rehabilitation efforts.

Human trafficking requires effective leadership, law enforcement, and legislation to protect communities and victims faced with this national security issue.

Due to enhanced legislation of the TVPA, previous cases of trafficking most likely would have been charged using weak and ineffective state statutes versus enhanced federal statutes enacted with TVPA legislation. Because priorities shift, some victims choose not to cooperate with law enforcement. Although state laws may be used to prosecute trafficking cases, laws prohibiting promotion of prostitution are normally weak and legislative language portrays trafficked victims as willing participants. The principal issue with current state laws is that they do not provide adequate protection for trafficking victims from additional prosecution – for example, under current state prostitution offenses, they could still be charged. Additionally, unauthorized immigrant victims – though afforded immigration protection through T Visas and U Visas, and Continued Presence – are potentially still hesitant to work with law enforcement for fear of deportation. Studies have yet to address the number of unauthorized immigrant victims that might have come forward had they had knowledge and confidence in U.S. Citizenship and Immigration Services efforts to assist them in prosecuting traffickers.

Prevention Measures

Media coverage continues to expand on stories of young women and children marketed and forced into commercial sex work in other countries. However, trafficking in the United States has traditionally received little attention until recently. Newly adopted federal legislation produces challenges for law enforcement and prosecution primarily due to the newness or nature of the crime, with no court precedence set. Because of this, several states have amended previous state laws to better address the issue locally – for example, the Florida legislature created the Statewide Human Trafficking Council in 2014.

Several causative factors of under-identification stem from lack of knowledge and awareness about the topic. Typically, victims have been treated as willing participants, with those illegally in the United States being deported. Raising awareness about human trafficking signs can be the most significant part of a prevention strategy. Globally, a critical prevention measure that nonprofits and governments have enacted and utilized has been awareness training. However, many trafficking victims are unwilling to cooperate out of fear of law enforcement and deportation, which makes identification and rehabilitation efforts difficult.

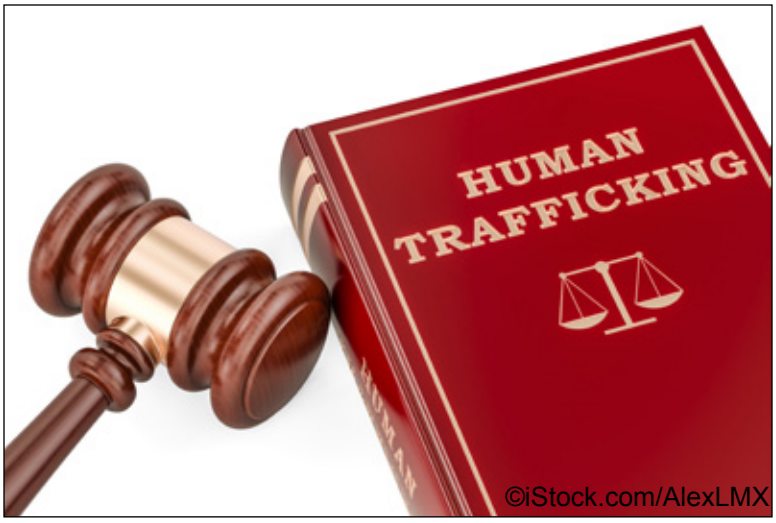
Ironically, with this lack of cooperation, few human trafficking prevalence studies have been conducted. Because there is a hidden nature regarding trafficking, all such studies rely on extrapolated data from other known sources. As a result, the exact magnitude of the problem globally, nationally, and within individual states remains a known unknown. In 2013, in an effort to address human trafficking, the U.S. government established the Federal Strategic Action Plan on Services for Victims of Human Trafficking in the United States 2013-2017, which focuses on four main goals:

- Align efforts of agencies;
- Improve understanding and awareness of the problem;
- Increase access to rehabilitative services; and
- Improve outcomes for victims.

In support of the Federal Strategic Action Plan – and in an effort to collaborate organizations addressing the issue – the Department of Homeland Security created the Blue Campaign that enforced and supported efforts to combat trafficking. The campaign creates a coalition or task force comprised of government and nongovernmental agencies, as well as private organizations and law enforcement, "to protect the basic right of freedom and to bring those who exploit human lives to justice."

In support for the Blue Campaign, on 21 June 2017, Senator Orrin Hatch (Utah) introduced the Public-Private Partnership Advisory Council to End Human Trafficking Act of 2017,

which established a public-private partnership and created the first ever Public-Private Partnership Advisory Council extrapolating knowledge and experience from government agencies and nonprofits to combat trafficking. The council serves as a single point of contact for program ideas and anti-trafficking efforts. It is comprised of 14 members from nongovernment agencies with extensive experience in anti-human trafficking, rehabilitation, and aftercare programs. Additionally, the same month that Hatch's bill was introduced, U.S. Senator Bob Corker (Tennessee) introduced the Abolish Human Trafficking Act and the Trafficking Victims Protection Act of 2017. These bills reinforce existing programs, provide additional resources to law enforcement, and enhance rehabilitative efforts for survivors of human trafficking.



A State-Level Call to Action

Over 50 new bills have been presented before U.S. Congress since January 2017 either introducing new legislation or addressing current legislation related to combatting human trafficking. Although federal laws have been enhanced, without a robust change to state laws and actions in addressing trafficking, federal government legislation will remain the primary authority in addressing trafficking crimes.

Federal laws enable law enforcement to target larger trafficking rings, but smaller trafficking networks in states typically go unaddressed either due to under-identification or inadequate state enforcement. Since smaller trafficking rings would likely be more identifiable to local law enforcement agencies, enhancing weak state laws would enable officials at that level to effectively address trafficking concerns. States with weak trafficking laws have a duty to implement more comprehensive laws that hold traffickers responsible and reinforce enhanced sentences for those convicted.

Trafficked individuals are victims – not criminals. Therefore, state legislation should strengthen tools to aid in prosecution, enact measures that protect and support victims, and enhance laws that are more punitive in nature. The TVPA is perhaps the most important piece of legislative law passed at tackling human trafficking because it demonstrates more punitive damages by implementing a 15-year to life sentence for those convicted. Unfortunately, the

TVPA applies only to federal cases. With that in mind, all states may have anti-trafficking laws, but not all laws are created equal.

Although all states have commercial sexual exploitation laws, most have not made it a priority to adopt strong penalties against trafficking. For example, Arkansas state law focuses punitive measures on the "John" rather than on the one who "forced and coerced" the person. The punishment currently for commercial sexual exploitation in Arkansas is a Class B misdemeanor for the first offense. Moreover, Montana has much more lenient jail sentences for traffickers compared to the TVPA – as the lowermost federal sentence is equal to the high-end state sentence in Montana.

According to Polaris, Florida ranks among the states with the toughest trafficking laws behind Delaware and New Jersey. Florida also ranks in the top tier states, which meet the criteria of laws critical to combating trafficking, punishing traffickers, and supporting survivors. In the United States, Florida ranks as the third busiest area for commercial sex trafficking. In 2015, Florida enacted new legislation focused on increasing penalties for human trafficking perpetrators, as well as providing additional protections for and protecting the personal identities of victims.

In an effort to end human trafficking, much more needs to be accomplished locally in states to complement the TVPA. Following the example of top tier states like Florida, Delaware, and New Jersey, enhancing state laws would enable prosecutors to better target traffickers. Additionally, measures are needed to protect victims of trafficking through measures that allow those who have been illegally trafficked into the country safe harbor and permanent residence, so they will not be reluctant to come forward and testify against traffickers. Moreover, trafficking awareness efforts should be enacted nationally in an effort to help identify potential trafficking victims.

Richard Schoeberl (pictured above), has over 22 years of security and law enforcement experience, including the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency's National Counterterrorism Center (NCTC). He has served in a variety of positions throughout his career, ranging from supervisory special agent at the FBI's headquarters in Washington, D.C., to acting unit chief of the International Terrorism Operations Section at the NCTC's headquarters in Langley, Virginia. Before these organizations, he worked as a special agent investigating violent crime, international terrorism, terrorist financing, cyberterrorism, and organized drugs. He was also assigned numerous collateral duties during his FBI tour – including a certified instructor and member of the agency's SWAT program. In addition to the FBI and NCTC, he is an author and has served as a media contributor for Fox News, CNN, PBS, NPR, Al-Jazeera Television, Al Arabiva Television, Al Hurra, and Sky News in Europe. Additionally, he has authored numerous articles on terrorism and security. He is currently a Professor of Criminology and Homeland Security at Martin Methodist College and works with Hope for Justice – a global nonprofit combatting human trafficking.

Benjamin Nivens has over 20 years of law enforcement experience serving as a Naval Criminal Investigative Service (NCIS) agent and a Tennessee law enforcement officer. Currently, he is an investigator and training instructor for Hope for Justice, a global nonprofit that investigates human trafficking and provides training to police and civilian entities. Additionally, he is a certified human trafficking investigator.

The Big Data Bind

By Daniel M. Gerstein

The use of genealogy websites to find the alleged Golden State killer, Cambridge Analytica's use of Facebook data to develop targeted ads for the 2016 presidential campaign, and the loss of privacy resulting from the sharing of information on social media bring into focus some of the unintended consequences of the collection, storage, and proliferation of personal information. The use of data in novel and unexpected ways pits users' demand for privacy against their desire to take advantage of the many benefits today's technology has to offer.

Increasingly, people willingly give up personal information and leave digital footprints that can be used in new and innovative ways for other than intended purposes. In some cases, personal privacy and even security are compromised. Personal data is sold as a commodity. Targeted "fake news" and advertisements are generated that infringe on users' online space. Users' daily movements and online activities are tracked and become part of digital profiles. Some personal data even makes it to the dark web, as one account offers, "The sale of stolen personally identifiable information is a growing industry on the dark web."

For users and policymakers, this sometimes murky digital landscape sets up a series of choices: if too much personal information is surrendered, privacy could be at risk; too little, and the benefits of emerging data technology could be lost. Striking the right balance could be the key to setting policy to maintain security while encouraging the safe deployment of existing technologies and the development of new ones.

By using free services such as Facebook, Twitter, and Google, users enter into grand bargains laid out in "terms of use" in which they consent to the use of their data for secondary purposes in exchange for access to the sites and the benefits that can be derived from social media and search functions. Such actions may incite the ire of average citizens when their personal information is compromised through big data applications, but informed users are willing to make the tradeoff nonetheless.

At the same time, though, promising opportunities could be squandered if restrictions are too strict or users become too restrictive with their information. For example, future autonomous vehicles – which could have potential to improve safety, ease traffic congestion, reduce the cost of transportation, and alter entire industries and car ownership trends – will likely depend on the constant exchange of information on location and position data with other vehicles, passenger requests and preferences, and traffic trends.

Personalized medicine potentially leading to improved quality of life depends on understanding the relationship between the human genome and the signals that regulate gene expression. It also depends on voluminous data sets on hundreds of thousands to millions of human DNA sequences. Armed with such knowledge, targeted drug delivery and perhaps gene therapies could contribute to the elimination of certain diseases.

Smart cities offer opportunities to create efficiencies for governments, industry, and individuals by eliminating redundancies, anticipating requirements, and improving city management strategies. But smart cities also rely on information technology networks, which allow for continuous exchange of information through the linking of sensors, flow models, and decision support tools to provide improved transportation, improved utility distribution, crime prevention, and traffic control to name a few applications.

To be clear, concerns about personal data privacy are not new, but they have become more pronounced as the magnitude of the potential loss of privacy comes into view. Congress and several states are taking up the issue and crafting legislation that would impose new regulations on companies that collect user data. The European Union has already acted on the issue with its General Data Protection Regulation, which requires important changes as a condition of use.

Understanding the limits on information sharing could be a first step. Identifying what data should be shared and placing limits on how long it can be accessed could be important. And identifying limits on the transmission of and uses of data by third parties could also be considered.

A balanced approach would be beneficial. To give some hypothetical examples: Autonomous vehicle data could be shared to ensure safety on the road, but not for developing personal profiles. DNA information could be used for assisting in personalized medicine, but not for making insurance coverage decisions. Smart city technologies could provide greater efficiency in people's daily lives, but not be used to infringe on individual privacy.

Ultimately, limits on collecting, storing, and proliferating personal information could be undertaken, but only with an understanding of the full costs and benefits of the use of such information. Identifying limits on unintended uses of personal data should be balanced against the potential societal benefits accrued through using this data. No doubt, difficult issues will be identified and will need to be addressed along the way. The first steps are to:

- Understand the acceptable limits of the uses of data; and
- Establish mechanisms to ensure that boundaries are not violated.

However, this dialogue should begin in earnest given recent trends.

Daniel M. Gerstein is an adjunct professor at American University. He was the undersecretary (acting) and deputy undersecretary in the Science and Technology Directorate of the Department of Homeland Security from 2011-2014.

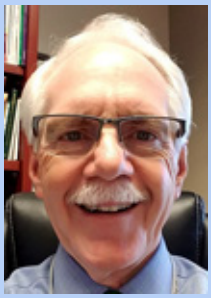
Public Health Preparedness: Segment 2

In 2017, many natural and manmade disasters affected communities across the United States. Each of these disasters posed many public health challenges, including funding, interagency, and workforce issues. Two subject matter experts from the Minnesota Department of Health and the Georgia Department of Public Health share their lessons learned from these disasters and provide insight on public health concerns that need to be addressed. This is Segment 2 of a two-part interview.

Click to listen to Segment 2.
(Segment 1 can be found here.)

Andrew Roszak, Moderator,
Senior Director for Emergency Preparedness, Child Care Aware® of America

Cheryl Petersen-Kroeber,
Director, Center for Emergency Preparedness and Response, Minnesota Department of Health (MDH)



Harry Bruce (Jeff) Jeffries Jr.
Deputy Director, Division of Health Protection, Georgia Department of Public Health

Three Ways AI Helps Prepare for Future Attacks

By Michael Ellenbogen

Terrorist attacks and mass shootings have changed the threat landscape. In the old-world paradigm, planes were the target and metallic objects were the key concern. In the new-world paradigm, anything can be a target. Thus, the security response needs to shift from reactive to proactive. Artificial intelligence (AI) is the key to moving from a reactive to proactive security response. Three specific applications of AI in the physical security field enable organizations to prevent attacks, not just react to them.

The physical security threat landscape has changed. Adversaries are no longer exclusively targeting planes, government buildings, and military facilities. Instead, they have expanded their list of targets to include special events, schools, shopping centers, transportation hubs, and sporting venues. Despite this expanded threat, many of these locations have not updated their legacy security technologies or shifted the procedures that are in place.

Although the ability to detect metallic threats is still important, traditional walk-through metal detectors were not designed to operate in large, open environments. With the purpose of detecting metal, such technologies often alarm on common items such as keys that do not present a threat. They also were not designed to detect improvised explosive device (IED) and other non-metallic threats. The all-too-frequent nuisance alarms, coupled with labor requirements and throughput constraints often make legacy technology difficult, if not impossible, to use. This then perpetuates the availability of soft, unprotected targets. With millions of people vulnerable to attack, a proactive rather than reactive approach using modern solutions is needed to prevent such incidents. Artificial intelligence (AI) can be implemented into a proactive approach in various ways.

Combating Emerging Threats

AI can be found everywhere. From companies using the technology to improve customer experience to hospitals using it to determine the likelihood of a patient being readmitted, the possibilities and applications are endless. However, in physical security, as the threat landscape continues to shift, a more mature, widespread adoption of AI is needed. As applications begin to take form, it is important to explore how this groundbreaking technology can be used to prevent future attacks on soft targets. Three AI applications that can help organizations take a proactive security approach to prepare for future threats include machine learning, object recognition, and faceless recognition.

1. Learning What Makes an Environment "Normal"

Machine learning (ML), an advanced form of AI that can be taught how to learn, can identify an object once characteristics are specified. Often referred to as environmental

awareness, this capability has proved beneficial for monitoring specific areas. By training the computer to learn what a "normal" environment is, it can monitor for anomalies and alert security personnel when something out of the ordinary occurs. For example, users can teach the computer what is allowed to be in a specific area at a certain point in time. Should the environment change, the computer would automatically alert that something is abnormal.

With computers taking on the responsibility of monitoring environments, guards and analysts can focus on higher priority tasks such as quickly responding to an actual threat. In addition, the element of human error is significantly reduced, as guards can focus on resolving specific alarms, rather than visually monitoring multiple video feeds.

Among the many uses of artificial intelligence, these three in particular could help soft targets better prepare for future attacks.

However, the introduction of new technology does come with increased false alarms. To help reduce false alarms, teams should customize the "normal" environment as much as possible while also clearly defining what "abnormal" factors warrant an alarm. The second application could be used to help avoid the system alerting unnecessarily.

2. Understanding What Qualifies as a Threat

In the same way ML can learn what is normal about an environment, it can also be taught to identify an object as something specific based on characteristics. This is referred to as "object recognition." In the situation above, users can teach the computer to only alert when people – as opposed to other objects such as animals, shadows, and windblown trash – enter the scene. This eliminates the system reacting to everything that passes through its field of view. With the right sensors, when surveying a large crowd of people, guards can determine if a visitor's bag might contain a threat object and then track that visitor or object. Should that person appear back on the screen without the bag, the computer can search the environment for the item, quickly sending security guards to that specific area and clearing the crowd.

In a security checkpoint scenario, this application eliminates the need for hand wanding or physical full-body pat downs as the technology itself would alert guards if someone is carrying an item of interest. Guards could then focus on a subset of people as opposed to screening thousands of visitors or travelers. This would also improve the visitor experience for all involved. Given current security systems are designed for specific environments, this capability allows security directors and teams to screen for a broader range of threats in a variety of environments, including stadiums, parking lots, and bus terminals.

3. Tracking Objects in Video Without Facial Recognition Capabilities

One application that is expected to gain traction is faceless recognition – also referred to as "object re-identification" – which is used to track an individual through multiple

fields of view from different cameras. With law enforcement teams often working from blurred and obscured images when identifying a suspect, this emerging capability is extremely promising despite its current limitations.

The ability to maintain awareness and track someone or something by its shape, clothing, or gait offers a powerful and potentially game-changing opportunity for security operations and attack prevention. Imagine the ability for law enforcement to employ AI on closed-circuit television feeds to track a known threat and detain suspects before they conduct an attack. Even more exciting is the potential synergies achieved by combining face and faceless recognition in tandem to optimize performance.

Researchers continue to make progress with this application, demonstrating that algorithms can be trained to identify people by matching previously observed patterns and mannerisms. However, performance improvements in faceless detection are still needed as false match rates continue to run high.

AI + Human Intelligence = A Worthy Opponent to Adversaries

From improving response rates to enabling pop-up security checkpoints, AI's adoption is making it possible for organizations to prevent attacks. However, it is important not to lose sight of the important role that humans play. AI has the power to analyze data quickly and identify patterns, but it cannot necessarily determine if these patterns are relevant. This requires insight and intuitive thinking, which is where the human brain performs best. It is the combined power of AI and human intelligence that will enable emergency planners and security personnel to combat today's new threat landscape.

Michael Ellenbogen is the CEO and co-founder of Evolv Technology. Prior to Evolv Technology, he co-founded Reveal Imaging and successfully led the company to achieve double-digit growth in both revenue and profitability since its inception. Through more than 20 years of contributions, he has reshaped the explosives detection industry. Reveal Imaging was acquired by Science Applications International Corporation (SAIC) in August 2010. Prior to Reveal, he was vice president of product and business development for PerkinElmer Detection Systems, overseeing the research and development, engineering, and marketing efforts. As director of marketing for Vivid Technologies Inc., he was instrumental in the transition following Vivid's acquisition by PerkinElmer. At both companies, he was responsible for market research, definition, and development of new products and product enhancements.

2018 Business Resilience Conference, Las Vegas, NV

By Rodger (Kevin) Clark

Natural and manmade threats and disasters face businesses today. Focusing on active shooter incidents alone, businesses are targeted more than any other entity. According to a 2014 FBI Law Enforcement Bulletin, between 2000 and 2013, most (45.6%) active shooter incidents occurred at businesses, with the next highest being education facilities (24.4%). To address these and other threats, business owners must have a continuity or emergency action plan that highlights mitigation, preparation, response, and recovery.

The 2018 Business Resilience Conference, organized by Continuity Insights, focused on providing business owners resources and ideas to develop a comprehensive business resilience plan. Selecting Las Vegas, Nevada, as the choice of venue after the deadly active shooter attack at Mandalay Bay was a profound decision by the conference organizers and demonstrated the seriousness of engaging business owners in a thoughtful discussion on business resilience. Conference presenters challenged business owners to think about not just operating a business but how to mitigate and manage the risk of operating a business. Some noteworthy topics presented included: decision-making strategies, risk management program development, crisis communications, social media and messaging, and response planning.

Mitigation

Mitigation is key to a sound business resilience plan. Mitigation activities prevent, reduce the chances of, or reduce the effects of unavoidable emergencies. Steve Jordan of Traiden Global Solutions engaged attendees on the importance of a deliberate Risk Management Program. According to Jordan, the most important part of the program is to have a plan. This begins by determining the risks and threats to the organization, and is followed by identifying vulnerable people and assets, developing a plan to rapidly deploy resources, and mitigating the event in a timely manner.

Although impossible to predict all possible disasters, developing a risk-based plan for an organization within a community and region helps to narrow the scope of the risk. As part of the planning process, Jordan stated that leadership must empower employees to offer suggestions and solutions that improve the company and secure jobs. After a risk management program is in plan, business leaders should work with all stakeholders in the organization to ensure they all understand mitigations in place and know what to do in a disaster. Continual development of the program is accomplished as required.

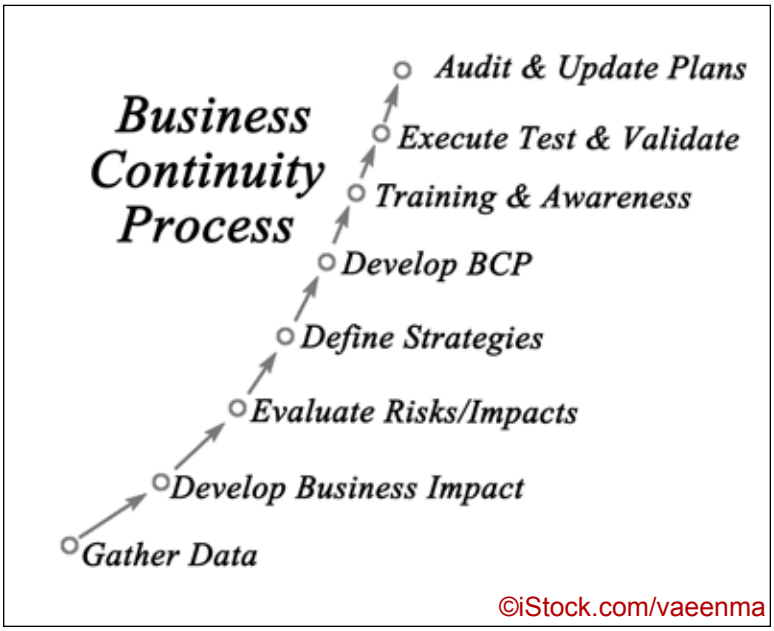
Preparation

The topic of active shooter was present during much of the conversations between business leaders and presenters. Bo Mitchell of 911 Consulting used his presentation on Fatal Flaws in Your Active Shooter Response to highlight the topic of preparation. Mitchell highlighted the importance of business leaders employing an emergency manager (EM) or business continuity (BC) person within their organizations. The EM/BC staff has the responsibility to implement emergency action plans, promote plans, exercise plans, conduct drills, and train company staff and CEOs. Mitchell noted that business owners must realize their most important asset is people, not revenue, property, intellectual property, or data.

According to Mitchell, the return on investment for businesses that spend funding and time to prepare and exercise plans is measured by the protection of people, protection of the brand, protection of productivity, protection of revenue, bonds employees into safety culture, build employee awareness, instilling a sense of responsibility, and increased employee ownership. People and businesses are naturally resistant to change, the EM/BC staff, who are on the frontlines of preparation, must become champions of change for the benefit of the company and its people. Their expertise should be sought after and utilized in any comprehensive business resilience plan.

Response

When disasters strike, individuals, businesses, and governments must promptly implement their emergency action plans and respond to save lives and prevent further property damage. James Powell of All Clear Fire Training noted during his presentation on the Anatomy of a Disaster that planning and exercising the plans before a disaster are the most critical elements of effective response. Powell then expanded on the types of disasters, National Incident Management System (NIMS) protocols, the disaster declaration process, community resilience, and how disasters start at the local level, which each serve as reminders to engage all stakeholders in the planning process.



Another topic that emphasized response addressed Social Media and Controlling the Message. Al Martinez re-

minded business leaders that perception is reality and how they can use communication channels to their advantage for crisis messaging. One takeaway is that sometimes prompt messaging on social media is appropriate, whereas other events do not call for a media release. Although the situation dictates the response, a decision-making process must be in place with leadership involved. Conference attendees gained new perspectives through examples demonstrating positive and adverse communication used in recent real-world events. For example, techniques used during events to generate automatic replies in social media venues show that an organization is engaged and responding to the event.

Recovery

After the disaster subsides, lives are out of danger, and the emergency is over, businesses transition toward a return to normalcy and begin repairing damaged property. The topic, Disaster Recovery, Removing the Mask of Mystery highlighted the importance of planning for recovery. The key when planning for recovery, according to presenter Sean Scott, Author of *Red Guide to Recovery and Secrets of the Insurance Game*, is to prepare for what is most likely to happen. Scott discussed the two types of people who emerge from disasters: survivors and victims. According to Scott, a little knowledge can make all the difference.

Individuals, businesses, and government agencies each need an awareness attitude before disaster strikes. Scott noted that business leaders must be aware of chemical and industrial hazards, price gougers wanting to sell services, and insurance claims processes. Disaster restoration is a multi-billion-dollar industry, and predators take advantage of those who are vulnerable. Business leaders should be prepared to provide counseling as needed for the grief of loss, financial strain, unemployment concerns, depression, suicide, and more. A recovery plan must be an element of an emergency action plan in order to provide a comprehensive solution to disasters.

The conference and workshops presented gave business owners many risk management and resilience tools to take back to their organizations to build on and improve their plans through the phases of emergency response: mitigation, preparation, response, and recovery. Overall, the tools and key takeaways from the 2018 Business Resilience Conference resonated well with attendees.

Rodger "Kevin" Clark is the co-owner and chief operating officer for C2 Threat Solutions, a veteran-owned consulting company specializing in solutions to high-risk threats. He is a retired Army police officer of 28 years and has over 29 years of security, emergency management, and law enforcement experience. He is recognized as an authority in law enforcement, security, safety and protection operations, doctrine writing and development, emergency management, physical security, antiterrorism, and continuity of operations planning. He is well-versed in strategic policy development and implementation, human resources and training management, large organization budget preparation, quality management and execution, and organization process improvement strategies. He has a B.S. in criminal justice and M.A. in emergency and disaster management. He can be reached via email at info@C2ThreatSolutions.com

WE STEPPED UP SO YOU CAN STEP BACK.

The new FLIR identiFINDER® R440 lets you scan for radiological threats from farther away to keep you and your community safe.

The new R440 is a lightweight, sourceless RIID that can be operated with one hand and is IP67-rated to survive tough missions. Not only does the 2x2 NaI detector deliver sensitive and fast detection, but it also provides accurate identification during secondary screening. The new 360° EasyFinder™ Mode expedites decision-making to keep you safe.

Learn more at flir.com/R440

FLIR identiFINDER R440
Highly Sensitive, Sourceless Handheld RIID

FLIR®