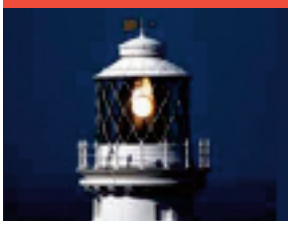


The Security Beacon

February 2021

Boston Chapter of ASIS International

In this issue...

www.asis-boston.org

Editorial: Howard Communication Associates
Design: MSG Design

2021 Security Expo Update

Mark your calendar for a great day of education, networking and connection in August

Hello ASIS Boston Chapter colleagues,

We have had to reschedule our wonderful Boston Chapter Security Exposition once again due to the pandemic monster. It was previously planned for April 2021, but we did not think we would be permitted to host a large number of people and we feared some individuals might not be vaccinated by that time.

The good news is we have been able to secure the new date of **Thursday, August 19, 2021*** for the 2021 EXPO at our venue, **Lantana's in Randolph**. The EXPO Committee is continuing to plan for this event and our hope is that we will break all records for attendance since we know how anxious people will be to get out, get some great education and do some much-needed networking. It will be so wonderful to see each other again so please put the date of **August 19, 2021** in your calendars.

CONTINUED ON PAGE 2

Soft target vulnerabilities in the 'new normal'

By Lawrence P. Smith CAMS, CFE, CPP, LPI

From a business standpoint, would you rather plan for a situation or event or react to it? Would you rather make a decision based on good information with time to prepare or newly discovered, rapidly changing information that hasn't been thoroughly vetted? The difference between your answer and what you've actually done when faced with these questions will play a key role in determining how your organization will do when faced with a critical incident.

For example, few businesses were prepared for the pandemic. Because of a failure to plan for the unexpected, many organizations are suffering right now in the "new normal." If you have to react to something you failed to identify as a threat or failed to plan for, such as a global pandemic, not only are you operating from behind, you are being forced to make decisions from a bad position. Such businesses are "soft targets," meaning their inadequate or lack of defenses make them an enticing target for fraud and potentially expose them to penalties for compliance failures. To avoid becoming a soft target and prepare for the next crisis, it's important to plan. Thankfully, it's possible to learn on the job during this current

CONTINUED ON PAGE 4

Chairperson's Message
Overcoming the trials of 2020, looking ahead to 2021

Hello and thank you for taking the time to check out the Boston Chapter of ASIS. As one of the oldest chapters in the US, the Boston Chapter of ASIS International prides itself on assisting security professionals from all industries and at all levels in developing and growing as security practitioners. Whether you've been in the industry for 30 years or are just entering the field, we hope to be a valuable resource in your professional journey. The relationships built, trainings held, and our certification prep courses are just a few of the ways we are here to support you.

The year 2020 was an interesting one to say the least, bringing us a host of unexpected challenges and uncertainties. Our Chapter responded with creative solutions, a lot of updates and a coming together to bring us through all that we endured. As we kick off 2021, we are seeing the fruits of those labors and a finish line in sight.

In 2020 the Boston Chapter was able to hold many virtual events where members, new and veteran, came together to discuss various topics, learn new things, check in with colleagues, and just say hi. Though we missed out on our 2020 Security EXPO, in 2021 we look forward to bringing back a live and in-person event. We also are having our first-ever Virtual CPTED course in partnership with the Toronto ASIS Chapter. Speaking of virtual, we are planning certification prep courses for CPP, PSP, PCI, and APP in the months ahead.

We look forward to collaborating with other ASIS Chapters and other organizations on bringing relevant content to our members. Your participation in what we have in store this year is eagerly anticipated and sincerely appreciated.

I would like to congratulate the rest of the 2021 Chapter officers. Paul Baratta has returned as our Vice Chairman; Kelsey Carnell has returned as our Secretary; and we welcome Larry Smith as our new Treasurer. I'd also like to thank Nick Biagioni who served as Treasurer last year and will continue this year as Vice Treasurer. I want to thank all of our hardworking committee chairpersons who put in a lot of time and dedication to ensure that our Chapter is moving in the right direction.

Our goal is still to sustain, grow and create a succession plan for the security industry here in Boston. This goal cannot be achieved without the participation, mentoring and collaboration of all of our members. Please stay in the loop with us and allow us to be a resource for you and your organization. Don't hesitate to reach out to us if you have any questions or would like to get more involved.

Thank you for your continued participation in the Boston Chapter.

Stephen Bertoni
Chapter Chair
ASIS International Boston Chapter

Sworn in as leaders of ASIS Boston for 2021 were (top row l-r) Kelsey Carnell, Secretary; Larry Smith, Treasurer; (bottom row) Steve Bertoni, Chairperson; and Paul Baratta, Vice Chairperson.

Asis Expo, cont'd pg 1

If you are a person or company who would like to exhibit at the EXPO, please sign up now by contacting Jim Stankevich jamesstankevich@gmail.com, or going onto the Boston Chapter's dedicated EXPO website. If you have other questions or suggestions, please reach out to me, bmichelman@partners.org, or anyone on the EXPO committee (Ashley Ditta, Jim Stankevich, Paul Baratta, Jennifer Goba, Craig McQuate, or Carolyn White).

I look forward to sharing more information about this event as we move into the Spring and really look forward to seeing you all this summer. Hopefully there will a lot of hugging happening at our August EXPO.

***I just want to remind everyone that this is all contingent on state guidelines for conferences and the status of the pandemic in August. If we are not able to do this fully in August, we will reschedule it again to the later Fall.**

Bonnie Michelman, CHPA, CPP
2021 Security EXPO Committee Chairperson

March

3

ASIS Webinar: Workplace Violence through the Five Phases of Emergency Management
11am-12pm
$49 members/ $79 non-members

More than two million American workers report being victimized by workplace violence which costs employers more than $120 billion a year. Our session will review workplace violence through the lens of all five phases of emergency management developing a workplace violence prevention program. For mitigation, employers need to identify risk factors for employees who may offend. For prevention, employers create a workplace zero tolerance policy for bad behavior that could lead to violence. For preparedness, training and exercises give muscle memory for employees to know what to do should they need to "run, hide, or fight." The business continuity functions of recovery should focus on recovery issues, such as crisis communications and post-traumatic stress disorder. Register at www.asisonline.org.

4

FREE Webinar: Stop Targeted Violence at Its Source: Threat Assessment and Management Basics presented by Dr. Stephanie Stein Leite
11am-12pm

We all want to stop future acts of targeted violence. This one-hour primer will introduce you to the world of threat assessment and management (TAM), the only preventative solution. Dr. Leite will teach you the difference between types of violence and expose you to basic threat assessment concepts. You will leave understanding the cornerstones of BTAM and the building blocks of developing, implementing and running a threat assessment team as well as with a host of resources to learn more about TAM. She will also describe how the Association of Threat Assessment Professionals (ATAP) can help you on your journey to decoding and stopping targeted violence at its source. Visit www.asis-boston.org for registration, login information.

9

FREE ASIS Webinar: Implicit Bias in Physical Security Operations: Why It Matters
3pm-4pm

The impact of implicit bias on physical security can have tremendous consequences. When a security professional must determine who is a threat or who belongs, their decisions and actions might be rooted in unwanted bias. Bias influences our perceptions about others, without our knowledge and consent — and is often misaligned with our personal beliefs and values about equality. It is critical for anyone interfacing with employees, customers, or the public—or anyone with oversight over physical security or a guard force, to be aware of how implicit bias affects our attitudes about others. Sadly, situations in which security professionals made biased judgments have resulted in tragic outcomes from job loss, reputational damage, lawsuits, and loss of life and human dignity. It's more important than ever for security leaders to be thinking about the role of implicit bias in our industry.

This webinar is presented as part of ASIS Member Appreciation Month and is free and exclusive to ASIS members. Register at www.asisonline.org.

16

FREE ASIS Webinar: Managing the Fear: Leveraging Emotional Intelligence to Help Fearful Clients Manage Crises
3pm-4pm

Effectively navigating a client through a difficult event requires more than just a firm understanding of crisis and threat management skills. Content knowledge is required, but not always sufficient. Beyond having content expertise, crisis and threat managers must also know how to emotionally engage and direct their clients so their crisis expertise can fully be utilized. How the crisis or threat manager handles those emotions, within themselves and within their clients, can make the difference between an effective or ineffective case outcome. Through case studies and video material, this session provides practical guidelines for understanding client emotional reactions, including how to effectively engage, understand, and redirect non-productive emotional reactions toward productive collaboration and case resolution.

This webinar is presented as part of ASIS Member Appreciation Month and is free and exclusive to ASIS members. Register at www.asisonline.org.

23

FREE ASIS Webinar: Strengthen your Organization through Business Resiliency
3pm-4pm

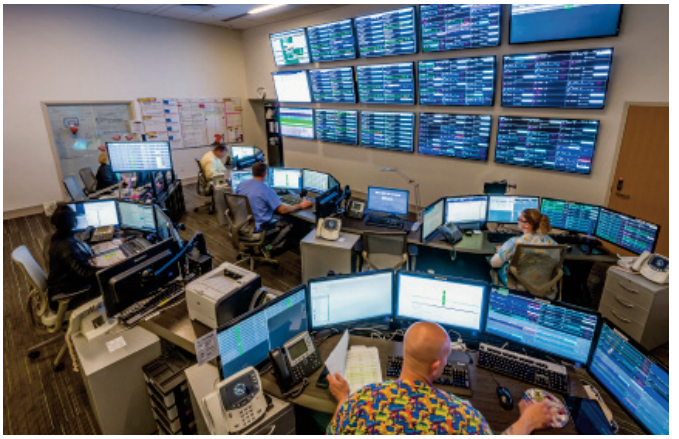
All organizations face emergencies and crises. The key is to accept and embrace those facts and build a Business Resiliency program to not only survive but thrive. This program focuses on three elements of Business Resiliency: Emergency Response, Crisis Management, and Business Continuity, and unpacks the mystery around how to develop the right plans to ensure preparation for the unexpected.

Attendees will participate in this webinar through polling and learn how each element can be simply addressed to build a formidable Business Resiliency program providing their organizations with a competitive advantage. Uncomplicated tools, techniques, and templates are shared so attendees can develop programs and customize plans. Register at asisonline.org.

This webinar is presented as part of ASIS Member Appreciation Month and is free and exclusive to ASIS members. Register at www.asisonline.org.

How can you use network surveillance to manage today's healthcare crisis and beyond?

By Paul Baratta



Over the past several months, facilities have dealt with many challenges trying to keep pace with the current health crisis. These have included the ongoing demand for personal protective equipment (PPE), exposure to COVID-19, the lack of critical medical devices, and the shortage of healthcare professionals. We can also add keeping staff, patients, and visitors safe, and PPE secure.

The myriad difficulties facing many healthcare systems raises the question: how can security professionals help healthcare providers meet the challenges they face?

In what's really a unique time in history, traditional healthcare measures may not always suffice. Many providers are turning to innovative ways to address the problems described above and pave the way toward improving patient care and enhancing safety and security.

One way they're preparing is by utilizing the latest network technology based on sight, sound and analytics. Today's network surveillance solutions are much more robust than legacy analog systems because they allow for greater flexibility and scalability, vastly improved image quality, and simpler integration, to name a few advantages. This can pay huge dividends for facilities by allowing them to do more even with limited resources. Let's discuss these challenges and how offering network surveillance solutions to your customers can help today and well into the future.

Remotely caring for staff

Healthcare providers can relieve pressure on their staff by monitoring and caring for patients remotely using a combination of network video, audio, and analytics. Network cameras coupled with analytics, for example, can identify specific sounds or motions that indicate distress. The solution can then alert staff of a problem and they can view the footage wherever they are and respond appropriately. A two-way audio feature would allow staff to remotely speak to the patient. By cutting down in-person visits or limiting staff rounds, facilities can help mitigate the spread of germs while still efficiently providing quality care.

One hospital in Orlando, Florida—Nemours Children's Hospital—has been using this type of tried-and-true solution for quite a while, even before the pandemic hit. And they've seen successful results.

Nemours developed a Tactical Logistics Center where a rotating team of paramedics continually observes patients' vital signs through a central monitoring system. Each room is

CONTINUED ON PAGE 5

SOFT TARGET, CONT'D PG 1

crisis and to adjust your operations for the next one. But first, let's consider the consequences when organizations fail to plan.

Planning for the unexpected

Making time-sensitive decisions based on unvetted information in a rapidly evolving situation is a recipe for disaster. You are going to have to expend capital to fix the issues that got you into the situation to begin with. Chances are your organization has also lost something of value that will need to be replaced, which will cost additional capital. That doesn't even begin to factor in all the ancillary costs that can be associated with becoming the victim of fraud or a compliance failure, such as the reputational damage, loss of existing clients, canceled insurance or increased premiums, the potential legal expenses, and the cost for a public relations firm to conduct damage control. Stock prices are typically affected when a company becomes a victim; what about the shareholders and their dissatisfaction?

If your business is facing a loss and you didn't – and perhaps still don't – have adequate risk mitigation measures in place, there is a distinct possibility that your insurer is going to try to find a way to avoid paying your claim. If they are able to show that you haven't been using industry best practices and enforcing your written directives, the insurer will likely decline to pay the claim based on your failure to take or enforce the necessary preventive measures to ensure the safety of an item of value. They also won't pay for your legal representation if you are sued by an investor. Instead, you may be forced to seek remedy through arbitration or a court of law depending on the language in the policy. Initially, there will be no payout at the end of that rainbow, and if you do win with the arbitrator or in court, it will be several months at the earliest before that victory. Then there is the appeals process, which will drag it out into at least the next year.

CONTINUED ON PAGE 5

Soft target, cont'd pg 1

As a security professional with decades of experience, including many years in law enforcement, what I find truly troubling is that despite the short-term inconvenience and minimal cost associated with deploying preventative methods designed to mitigate risk, establishing and maintaining industry-specific internal controls and training your people, organizations are still sacrificing safety and security for greater profits. There are very few situations in which you can't prevent something from happening or find a remedy if you have the foresight to plan accordingly. Managing risk is about understanding value, protecting that value and adapting as the landscape changes. Yet, to avoid all the costs I just mentioned, companies seem to prefer to react to crises after the damage has been done. There's a better way.

Understanding what makes something valuable

Now that we've established why planning is important, the first step in risk management is understanding and identifying what is of value. Everything has value to someone, even if you don't see it yourself. Whether the value is subjective, such as with art and fashion, or contextual, such as the scaled-up economics of a single cup of coffee for a single person versus the coffee budget for an entire corporation, it's critical to recognize the importance and shifting dynamics of assigning value.

Some things are inherently valuable because they constitute a commodity like gold, silver, and diamonds. Other things have value because of supply chain limitations that can cause the intrinsic value of an item to surge. Think about how the public reacts to scarcity of the products and services they want or need. The hottest new holiday toys are often sold at a premium and then re-sold on the black market at a steeper premium. When people believe the supply chain is going to be disrupted, oil prices soar. After natural or manmade disasters, like Hurricane Katrina and the Deepwater Horizon explosion, oil prices spiked. Intentional acts can have the same effect. During the oil embargo in 1973, the Organization of the Petroleum Exporting Countries (OPEC) reduced oil exports to gain leverage on countries supporting Israel. It resulted in gas rationing and prices spiked by 400%.[1]

When thinking about the assets that provide value, companies often overlook and underappreciate their employees. As valuable as employees are, they are also a company's biggest vulnerability. Onboarding and vetting a new employee is expensive and time consuming.

[A]ccording to the U.S. Department of Labor, the price of a bad hire is at least 30 percent of the employee's first-year earnings. For a small company, a five-figure investment in the wrong person is a threat to the business.[2]

Your responsibility as a leader is to protect your employees and provide them with a safe workspace. That same philosophy should extend to your vendors, customers and clients. Employees who feel safe and appreciated are far more valuable than disgruntled workers who may leave the company – or worse.

The second part of risk management involves a two-pronged approach. First, you must develop a plan to ensure the safety and security of your employees. Next, you must rank your

continued on page 6

[1] https://www.livescience.com/44282-opec-oil-embargo-40-years-later.html

[2] https://www.forbes.com/sites/falonfatemi/2016/09/28/the-true-cost-of-a-bad-hire-its-more-than-you think/#5d09681f4aa4

Network Surveillance, cont'd pg 4

equipped with a camera. To ensure privacy, the camera's field of view is limited to the patient's bedside and only turned on after paramedics call into the room. A red light on the camera then flashes when it's live streaming.

This kind of network surveillance solution can eliminate false alarms and help paramedics better determine non-events, which don't warrant an emergency response. For Nemours, their system also helped the team prevent a sick teen from leaving the building. By utilizing network cameras, staff at Nemours (and other hospitals) can rest assured that if they do /visit a patient and leave the room, they're not actually leaving him or her unattended.

Protecting patient health and securing medical equipment

Patient safety is obviously of the utmost importance. But a surge in hospitals can put patient safety and security at risk. For example, when hospitals went into lockdown earlier this year many reduced the number of entry points to one main entrance so they could screen all incoming visitors.

An access control solution can help facilities more easily monitor everyone who enters the building as well as when and where they enter. For example, network cameras coupled with crossline analytics (a trip-wire application that can be installed on the cameras) can trigger an alert to personnel or prompt a network speaker to play a pre-recorded clip asking visitors to proceed to a specific entrance for screening.

Providers can also use low touch access control to allow authorized people to enter a building or area but mitigate the spread of contagion by reducing the number of touch points. Or it can be paired with another third-party system that enables doors to automatically open and close to eliminate major touch points upon entry.

continued on page 7

Soft target, cont'd pg 4

company's physical assets according to their value and likelihood that they would be stolen, reverse-engineered, copied, or forcibly kept from you (think ransomware). You need to know what makes your assets valuable to you. Just as importantly, you need to know what makes them valuable to someone else. Understanding that internal and external value allows you to begin to put together a plan to protect those items. You can't protect the item of value knowing only one side of the equation.

Protecting the value

For anything with value, there is someone willing to take it. When thinking about potential vulnerabilities the biggest weak point comes from people with access to your assets: employees, clients, customers, contractors, vendors, visitors, and consultants. The number one thing a company can do to protect its assets is to have a proper set of internal controls.

Internal controls are the policies, procedures, rules, and regulations incorporated into your operational documentation and employee handbooks. For example, internal controls may include procedures around change requests, ID verification, documentation requirements and procedures, governance around data control and access, and tools and technology to promote physical security.

Companies that have a proper set of internal controls have invested time and money into creating a system that sets the parameters for handling anything they had the foresight to address. According to the 2020 Association of Certified Fraud Examiners (ACFE) Report to the Nation, a third of fraud is directly attributable to a lack of internal controls.[3] If a company became a victim despite having a set of internal controls, it was likely because management failed to enforce or update them. Your policies, procedures, rules, and regulations are only as good as the people who monitor and enforce them. If no one is being proactive to ensure people are adhering to the existing policies, then those policies aren't worth the paper they are written on.

With these facts in mind, to foster a culture of compliance, assign ownership of every internal control to the managers and supervisors you expect to enforce their usage. Periodically assess the degree of compliance with every control. If employees fail to follow them, or management fails to enforce the internal controls within their area of responsibility, consider disciplining those involved. When a control breakdown happens, make sure there's a remediation plan in place, with clear ownership of tasks and a timeline for their completion.

The 'new normal'

So far, COVID-19 has affected over 95.8 million people and killed 2.05 million globally. Of those, the United States has had more than 24 million cases, of which 399,000 resulted in a death. No country was properly prepared for this situation. And, as we've already noted, few if any businesses were prepared, but all of them should have known that something like this was possible.

From a risk management standpoint, the threat must have been deemed minimal, as nearly all countries and agencies opted to allocate resources to more-pressing or seemingly more-plausible matters. It is still too early to know exactly what the long-term ramifications of this virus will be. Nonetheless, this crisis and every crisis that follows will bring new forms of risk to light, providing companies with the opportunity to uncover new ways to manage those risks.

What I can tell you is that COVID-19 is a catalyst for societal changes – some good, others that will undoubtedly be met with protest. As industry experts, we need to think outside the box to help businesses of all sizes get back up and running, keep their employees, clients, customers, contractors, and others physically safe, and protect their other valuable assets.

The widespread use of masks has presented new opportunities for crime, big and small. A growing number of robberies involve masks, and minors have started scamming liquor stores by wearing masks and "aging" themselves up with makeup and talcum powder.[4] [5] The consequences of mask-wearing extend beyond the moment of the crime. Masks often nullify facial recognition software and prevent law enforcement from using security camera footage to identify a robber. If liquor stores get caught selling to minors, they will face fines, suspensions, revocations of licenses, potential lawsuits by parents, reputational damage, and the loss of their insurance policy. On the other hand, if you ask someone who's particularly vulnerable to the disease to take their mask off as a security precaution, it has the potential to increase their exposure to the virus. I could see a suit coming from a violation of the American with Disabilities Act for failure to accommodate.

…companies must be proactive and identify potential vulnerabilities as the 'new normal' presents them.

Furthermore, businesses have the unenviable task of trying to protect their employees and their customer base from exposing themselves and each other. They also have to ensure that they are adhering to the regulatory agencies that govern their operation. For example, many industry sectors already have stringent identity verification procedures. Banks, for example, scan your license and keep it on file; cannabis facilities scan an approved ID just to let you in the building; and medical facilities require ID and your insurance card before you are seen by anyone – all that before the addition of masks. With millions of employees forced to work from home for the foreseeable future, we're seeing changes in the threats fac-

CONTINUED ON PAGE 7

[3] https://www.acfe.com/report-to-the-nations/2020/

[4] https://q1065.fm/when-buying-alcohol-customers-may-be-asked-to-remove-their-masks/

[5] https://www.foxnews.com/us/teens-are-dressing-up-as-mask-wearing-grandmas-to-score-alcohol

Soft target, cont'd pg 6

ing companies and their employees. For example, there's been a significant increase in email scams related to the virus, including those designed to help criminals breach a company's security defenses.[6]

The widespread use of masks and other factors have presented a changing landscape and it's necessary to react accordingly in order to mitigate and manage risk. While no one has all the answers yet, companies must be proactive and identify potential vulnerabilities as the 'new normal' presents them. They must continue to identify, assess, and prioritize issues of concern and then implement the appropriate mitigation programs to address those concerns. These mitigatory steps take into account cost, time, availability, vulnerability, risk, and a few other industry-specific issues. Once a company identifies the appropriate countermeasures, it can begin the deployment process. If they can't address all of the issues right out of the gate because of cost, executives should factor these deployments into a three- to five-year capital improvement plan, then stick to it.

Suggested solutions to mitigate soft target vulnerabilities

With all of that said, what if you want to start taking steps today to avoid being a soft target? Here are some suggestions that have helped many of my clients shore up their defenses.

• Update internal controls

If you haven't already amended your internal controls to address a future pandemic, I suggest you start there. Examine the knowledge and methods you have learned as a result of this current pandemic. Keep the things that have been successful and dump the rest. If you are unsure about the legal ramifications of updating your internal controls to address this issue, contract it out.

continued on page 8

[6] https://www.infosecurity-magazine.com/news/phishing-bec-covid19-attackers/

Network Surveillance, cont'd pg 5

From a security and operations standpoint, an access control solution ensures facilities are always in complete control. They can grant people access with a specific type of identification method or simply revoke or change their access as needed. These solutions are also perfect for securing areas within a building that house PPE or other medical equipment.

Network solutions aren't limited to permanent fixtures. They work in temporary structures as well. As you're probably well-aware, earlier this year many hospitals set up temporary structures to care for an overflow of patients with COVID-19. Due to the high cost of traditional security measures, there's always risk these structures could be left inadequately secured, making it difficult to keep patients and staff safe and PPE secured. But that's where the power of integration comes into play. In some cases, because of the open architecture of the network cameras you can easily integrate existing systems, such as parking lot cameras, with new network audio and access control devices. A deployable solution is extremely advantageous because it's relatively quick and easy to install and adapted to provide a reliable and scalable surveillance system.

Network solutions for today and tomorrow

Hospitals will continue to face new challenges as they cope with the ongoing health crisis and they will certainly need to adapt and evolve to meet new ones that arise. Network surveillance systems are the perfect solution to offer your customers to help them manage their immediate needs, such as mitigating the spread of germs and maintaining a secure environment. But they're also long-term answers to meeting tomorrow's demands and uncertainties in the emergency situations that lie ahead.

ASIS Boston Vice Chair Paul Baratta is Business Development Manager for Healthcare for Axis Communications.

Jumpstart your security career

Broaden your horizons by becoming a Certified Protection Professional (CPP), Professional Certified Investigator (PCI), Physical Security Professional (PSP), or Associate Protection Professional (APP). **ASIS Boston** will offer virtual certification prep courses for all four credentials in the months ahead. Learn more at **ASIS Boston** or by contacting Certification Chair Craig McQuate, **craig.mcquate@takeda.com**.

Send Us Your News!

Share your knowledge of the security industry by writing for *The Security Beacon*. Email articles and photos to: **rzupan@enesystems.com**

Soft target, cont'd pg 7

• Assure legal compliance

Before implementing any major changes, make sure to speak with your legal team to find out what your obligations are under Occupational Safety and Health Administration (OSHA), Equal Employment Opportunity Commission (EEOC), Massachusetts Commission Against Discrimination (MCAD), Health Insurance Portability and Accountability Act (HIPAA), American with Disabilities Act (ADA), and/or the Rehabilitation Act. The EEOC is preparing for a surge in the number of claims as a result of the pandemic, and they have provided guidance documents and published *Pandemic Preparedness in the Workplace and the Americans with Disabilities Act*, which was updated as of March 21, 2020.[7]

• Be creative

OSHA requires you to provide a safe space for your employees as well as your customers. Because of the unique nature of a pandemic, people are wondering how to protect both. This is where thinking outside the box will be a benefit. Rather than reinventing the wheel, try to use existing technology along with some administrative changes and training to adapt to new risk management, security, and fraud-related issues.

As I've pointed out throughout this article, you can improve your planning by being adaptive during a crisis. By addressing short-term vulnerabilities in the midst of a crisis, your organization will be safer, more secure, and thus better able to weather a subsequent crisis. If nothing else, it will show what your company can accomplish when the threat landscape changes in significant and previously unimaginable ways.

[7] https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act

Case Study: Banking Solutions for Identity Verification During a Pandemic

When considering how to adapt to the shifting conditions of the new normal, let's take the example of a bank. When trying to solve new problems, organizations can often be creative with existing resources. For banks, in many cases, the technology to solve these new issues already exists. Furthermore, the price point for the software and hardware has come down since their introduction, making it affordable for all banks, regardless of size. Here are just a few ways an organization like a bank could implement existing technology to solve an emerging threat.

• Dual-factor authentication

Banks already use dual-factor authentication for ATM transactions: you are required to have an ATM card and a personal identification number. To enter the bank, the client would have to present their bank card and complete a biometric verification process. Once the identification process is complete, the door unlocks, and the customer can enter the bank. If they refuse to participate in the required dual-factor identification process, they can use the drive-up window instead. If you don't have one, install one.

• Unique identifiers

Banks can also require a thumbprint for teller transactions. You can also ask customers to verify some recent transactions that were made on their account. Establish a single word challenge that only the person who opened the account would know, eg. "Question: Sir, can you please advise what your challenge word is? Answer: It is Tiger." There are plenty of ways to establish unique identifiers that can be used to verify an identity.

• Access control

Don't allow non-bank clients into the bank; mandate they use the exterior option. By doing this you have limited the opportunity to rob your organization. You have taken away the robber's ability to use the interior of the bank to hide his actions. Drive-up windows are in plain view for the public or the police officer driving by to see. Bank drive thru and exterior walk-up windows don't typically get robbed for those reasons. Let's not forget the physical distance, the cement wall and bullet-proof glass barriers which are also deterrents.

I hope you were able to take away two lessons from this article. First: prevention is always more cost effective than becoming a victim. Second: taking action today to assess the landscape and improve your defenses can help prevent your organization from becoming a victim in the future.

If you are ready to get started on creating a crisis response or business continuity plan for your organization don't hesitate to reach out to us. Our business model affords us the luxury of sharing our cost savings with the client without sacrificing on the service. Can you really afford not to give us an opportunity to keep you off the front page?

Stay safe and keep an eye out for the recently finished and soon to be released White Paper titled, *Moving Beyond the Use of Barcodes in Property and Evidence Management.*

ASIS Boston Treasurer Lawrence P. Smith, CAMS, CFE, CPP, LPI, is the CEO and founder of The Stirm Group. He has authored several articles on fraud and security related matters. His article on the "Victimization of the Massachusetts State Police," was published in the November/December 2018 issue of Fraud Magazine.