DomPrep Journal

Disaster Support

Volume 17, Issue 8, August 2021

Since 1998, Critical Information for Preparedness and Resilience

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

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

Dräger

Teledyne FLIR

PROENGIN Inc.

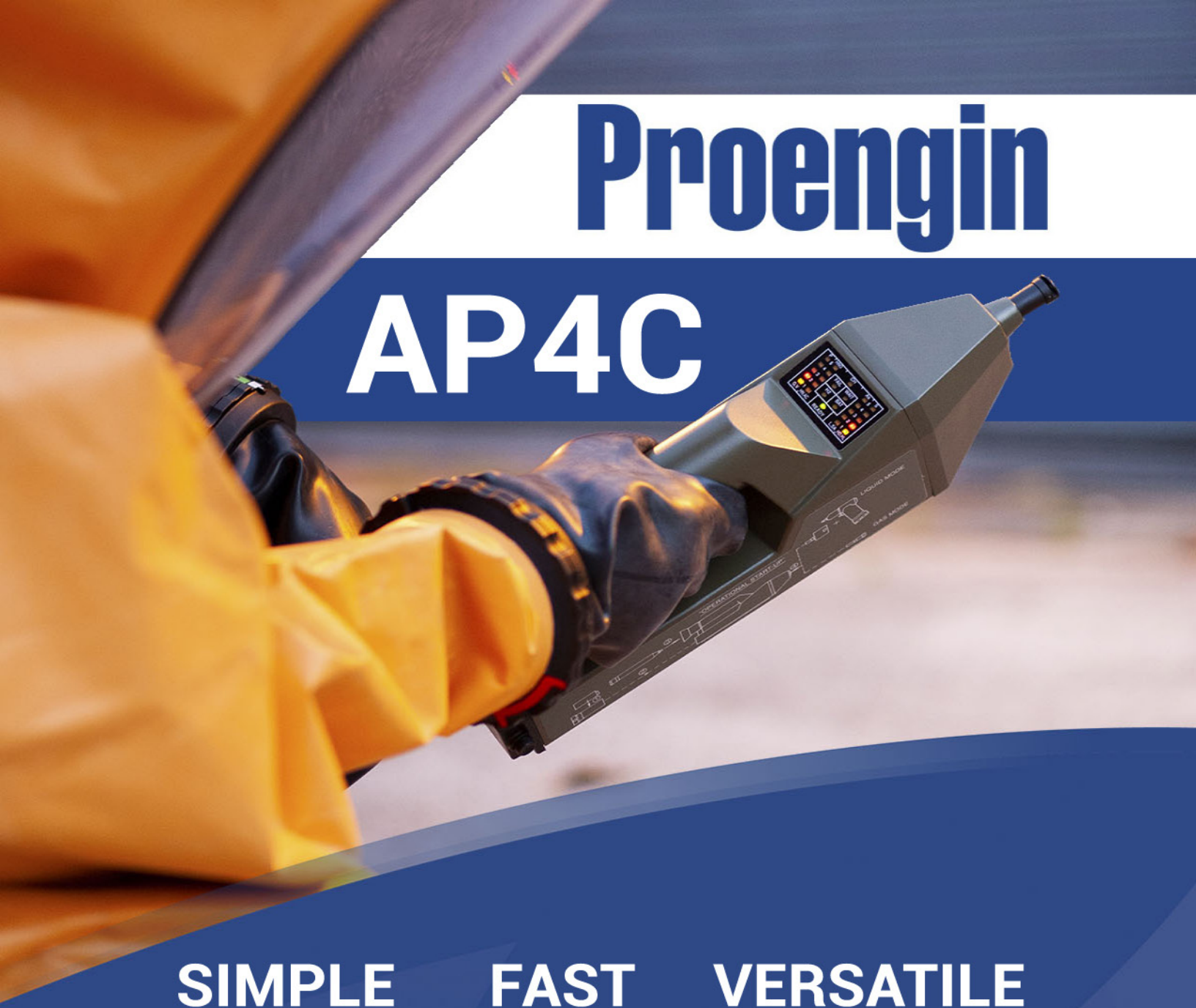
DomPrep Journal is electronically delivered by the IMR Group Inc., P.O. Box 810, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomPrep.com

Featured in This Issue

Pictured on the Cover: Fairfax OEM (Virginia), 2021

Proengin

AP4C



SIMPLE FAST VERSATILE

Chemical weapons & NTAs

HAZMAT & Homemade agents

Quick response

Accurate & Precise

www.proengin.com

Different Sides of Disaster Support

By Catherine L. Feinman

Disaster support often conjures the image of boots-on-the-ground responders providing aid to survivors on scene. However, disaster support involves so much more that is accomplished at each phase of the disaster management cycle. These efforts include creating codes and standards, building a workforce, providing financial aid, and offering psychological support.

One way to mitigate threats is to ensure that building codes and standards are in place and inspections and repairs are conducted and enforced. Even in areas where current building codes can withstand destructive winds, earthquakes, and other disasters, older structures may require updates to address evolving risks and threats and save lives. For example, in June 2021, the lives of 98 Surfside, Florida residents were lost in a condominium collapse despite warning signs of structural deficiencies.

Since all disasters cannot be mitigated, communities must prepare for numerous possible threats and hazards. This process begins with people who can fill the many staffing requirements within agencies and organizations. During COVID-19, many people were sent home – some able to work remotely and others who lost their jobs. As operations rebuild, emergency preparedness projects such as internships and trainings have restarted to help fill critical current and future human resource needs.

In the aftermath of a crisis, response can be seen in the form of physical, virtual, or financial efforts. During COVID-19, large sums of money were distributed across the country to provide critical financial aid to those in need. Unfortunately, criminals also responded to the pandemic by taking advantage of opportunities through efforts such as financial fraud. These types of compounding events create even more challenges in the days, weeks, and even years that follow.

Of course, there is no timeframe for the recovery phase. The communities' actions within the other three phases could shorten or lengthen the recovery period. Even then, some disasters may require a lifetime of recovery from the physical and/or psychological effects on survivors. Regardless the stage of the disaster, there is massive support that DomPrep readers and others provide before, during, and after disasters. This issue of the *DomPrep Journal* is dedicated to all those who serve in these critical roles.

Emergency Management Projects in a Quasi-Pandemic World

By Sarah Keally

The COVID-19 pandemic put many projects on hold and stalled efforts to build the workforce and train the next generation. Now that agencies are revisiting pre-pandemic projects, the Fairfax County Office of Emergency Management in Virginia offers a best practices approach for introducing internship programs and filling critical operational and resource gaps.

The Fairfax County Office of Emergency Management (OEM) in Virginia usually hosts one or two interns a semester, selecting them through a competitive interview selection process. The internship program is structured to help them take on actual projects with deliverables and cumulates in a final capstone project that is presented to the office on their last day. In addition to their projects and deliverables, the internship program is designed to give them exposure to all the different aspects of the emergency management office and field. They have a sit down with each of the divisions – Planning and Policy Analysis, Mission Support, Technical Services, Training and Exercises, Continuity of Operations Planning, and Community Engagement – to orient them early in the program. Then they learn, through trainings, meetings, and their projects, the different phases of emergency management and how a local government office operates in a large urban area. They also receive overall general career and professional development opportunities.

Lockdowns & Restarts

Due to the COVID-19 virus pandemic that brought lockdowns to Fairfax County and much of the world in March 2020, the office suspended the internship program until case transmission rates decreased and vaccination rates were at a relatively high rate. As things slowly started opening again in the spring and summer of 2021, it was decided to allow interns to support OEM again. OEM selected two interns for the summer 2021 session, one from an undergraduate Geographic Information System (GIS) program at Mary Washington University and a second from a graduate program from Penn State University's online Masters of Homeland Security program. Interns typically work 20 hours a week in the office to ensure they have sufficient time to work on projects and attend meetings as needed.

As the COVID-19 pandemic response transitions to a mitigation and recovery effort, projects that were put on hold can resume, including internships.

Based on their career interests and the office project needs this summer, OEM assigned them projects related to training and exercise development, GIS map and tool building,

Emergency Operations Center (EOC) guide documents, and their capstone project, which has significantly more requirements than their other assigned projects. To complete the capstone, the interns must work together to formulate a plan for completion, delegate the work among themselves (if there is more than one), coordinate with the relevant staff to ensure the deliverable will meet the needs, and then present on their methodology, research, lessons learned, and the product itself at the end of their semester session with the office.

Capstones, Projects & Guides

This summer's capstone project was to transition the Multi-Year Training and Exercise Plan to a Multi-Year Integrated Preparedness Plan. The new integrated preparedness plan format would allow for more integration of the local planning and operational goals and objectives to help drive the training and exercises needed to prepare county staff and partners over the next several years. The two interns presented their process for developing and writing the plan, which they created from reviewing similar plans in the National Capital Region and other local emergency management programs across the United States.

They learned how to professionally format the document, suggested what elements to include and what did not work, what would need to be added to the plan in the future, and how to gather the information needed to develop it by collaborating with other staff in the office. The interns produced a nearly finalized plan. The Planning and Training and Exercise division staff will add the priorities and capabilities that need to be addressed with input from internal and external agency partners as part of the Integrated Preparedness Planning Workshop scheduled for Fall 2021.


Fairfax OEM (Virginia), 2021

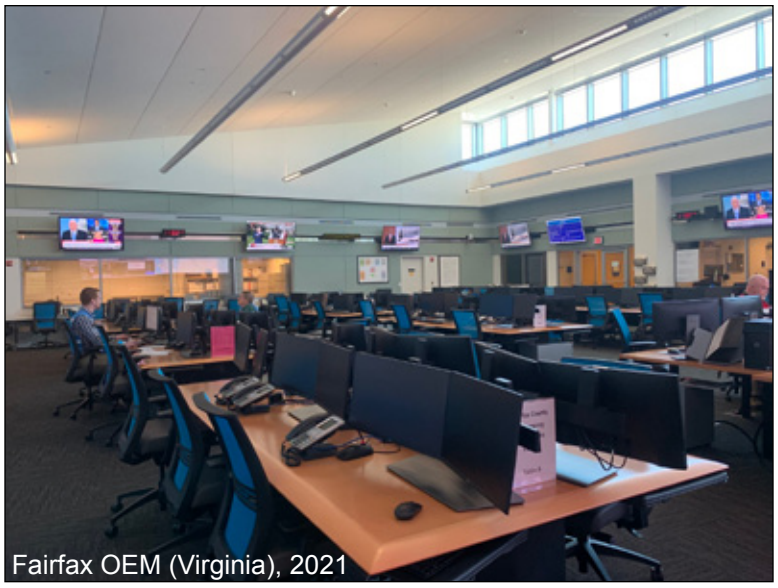
In addition to their capstone project, the interns have also worked on creating and updating EOC placemats for at least twelve positions in the EOC, starting with EOC Command and General Staff positions, to help serve as quick reference guides for those working physically or virtually in the EOC. The placemats have an organizational chart, or a flow chart, on one side as an easy visual reference then several bullets of actions or decisions to make for each phase of the EOC activation shift. These placemats will be handy references for future activations.

Another project that will be helpful to businesses in Fairfax County is the business version of the Community Emergency Response Guide (CERG). The guide was designed to help

residents, communities, and businesses be better prepared and even mitigate certain hazards that frequently affect Northern Virginia and the surrounding National Capital Region. The CERG and its associated templates – along with hazard webpages designed to help the public prepare for, mitigate, respond to, and recover from the hazard – are located on the Fairfax County website. The Business CERG is about 80% complete with the help of the interns and will be completed soon to share with the local Business Emergency Operations Council and other business leaders.

Future Plans

As the COVID-19 pandemic response transitions more to a mitigation and recovery effort in Fairfax County, OEM can resume projects that were put on hold. This will help develop internship projects for the next semester once the next set of interns are selected. The Planning and Policy Analysis Division is currently working on a new Alert and Warning Annex to supplement the Emergency Operations Plan and put an emphasis on equity.


Fairfax OEM (Virginia), 2021

Many of the OEM's plans are currently being reviewed and potentially revised with more of an equity lens with help from partners to ensure the OEM is better able to address the needs for all residents. The next set of interns can provide a fresh take on topics rising to the top of the priorities list such as equity in all phases of emergency management, virtualization of the EOC and its functions, and impacts of climate change. In the future, the agency will incorporate more of that in all phases of emergency management and in the utilization of the funding received to support those efforts.

Sarah Keally has over 12 years' experience in the emergency management field. She currently works for the Fairfax County Office of Emergency Management (OEM) as an emergency management technical specialist. She is the county's WebEOC and Everbridge Alerting System administrator as well as responsible for many of technology solutions supporting the emergency management program and Emergency Operations Center (EOC). She currently serves as the National Capital Region WebEOC Subcommittee chair and advises the Metropolitan Washington Council of Governments (MWCOG) Emergency Managers Committee on the crisis information management needs for the region. She came from the Fairfax County Health Department Office of Emergency Preparedness where she spent four years as the emergency management specialist responsible for managing grants, logistics, communications, planning, responder health and safety, and as Duty Officer program. She has worked in public health emergency preparedness since 2008 and transitioned to emergency management in 2017.

Building Codes Support Disaster Preparedness & Resilience

By Karl Fippinger

Building codes and standards have long been a silent partner in the health, safety, and welfare of communities and are becoming increasingly more important in society. Today's emergency managers and community leaders face a multitude of risks including extreme weather events such as hurricanes, tornados, straight-line winds, flooding, drought, and wildfires, as well as global risks from communicable disease outbreaks and environmental change. Luckily, building codes and standards continue to provide a safe structural foundation for communities as a trusted and proven resource and are regularly evolving to meet the challenges of these dynamic threats.

Modern building codes and standards offer communities both a foundation and framework for increasing their resilience through a variety of tools and resources that can be applied across all four phases of emergency management – mitigation, preparedness, response, and recovery. To reap the benefits and increase their communities' resilience, emergency managers and community leaders must push for the adoption, implementation, and enforcement of the latest building codes and standards.

Protecting Community Lifelines

One of the most effective ways to increase community resilience is by mitigating risks to one or more of the Federal Emergency Management Agency's (FEMA) Community Lifelines. These lifelines enable the continuous operation of critical businesses and government functions and are essential to health, safety, and economic security. Model codes, such as the International Codes (I-Codes) – a family of 15 coordinated, modern building safety codes used in all 50 U.S. states and in many other countries – are vital to the protection of these lifelines as they safeguard against disasters like fires, weather-related events, and structural collapse.

For example, the codes have provisions for adopting, developing, and strengthening requirements for land use, zoning, floodplain management, infrastructure, or fire-resistant construction in the wildland urban interface (WUI), which are critical to mitigating damage from wildfires. The I-Codes underpin the most basic of community lifelines including food, water, and shelter, the construction, maintenance, and operation of health and medical facilities, and the safe storage, conveyance, and use of energy, fuels, and other hazardous materials.

Adopting Modern Editions of Building Codes and Standards

When disasters strike, building codes and standards serve as a baseline for the return to safe, sanitary, and habitable buildings. Most communities have adopted at least some minimum codes and standards for buildings, fire prevention and life safety, plumbing, mechanical, zoning, and others. However, according to FEMA, only about a third of U.S. communities facing damaging wind, hurricane, tornado, seismic, or flood hazards have adopted hazard resistant codes. In addition, ISO/Verisk's 2019 National Building Code Assessment Report found that only 16 out of thousands of counties and cities in the U.S. achieved a top score, and nearly half of states do not mandate building code enforcement statewide.

Yet, the National Institute of Building Sciences (NIBS) in its Natural Hazard Mitigation Saves: 2019 Report found that adopting up-to-date editions of the International Codes (I-Codes) generates a national benefit of $11 for every $1 invested. The NIBS report also highlights a national mitigation benefit-cost ratio associated with code adoption of $6 to $1 for riverine and coastal floods, $10 to $1 for hurricanes, $12 to $1 for earthquakes, with benefits as high as $8 to $1 for wildfires through avoided casualties, post-traumatic stress, property damage, business interruptions, and insurance premiums.

Only about a third of U.S. communities facing damaging wind, hurricane, tornado, seismic, or flood hazards have adopted hazard resistant codes.

Understanding this, FEMA has called adopting current building codes "the single most effective thing we can do," and incentivizes, through grants and as a project scoring criteria, the use of building codes and standards in its grant programs like the Building Resilient Infrastructure and Communities (BRIC) program and its other hazard mitigation assistance grant programs. Emergency managers and community leaders are encouraged to take full advantage of federal, state, local, tribal, and territorial hazard mitigation assistance grant programs to help mitigate risk using codes and standards.

Leveraging Governmental Aid

Code officials and their floodplain management counterparts rely on support from emergency managers and community leaders to help secure the critical resources needed to ensure the health, safety, and welfare of the community. To that end, FEMA recently announced a new disaster policy specifically aimed at providing much needed assistance for code officials and floodplain managers during disaster response and initial recovery for up to 180 days following a major disaster declaration. The policy, administered under FEMA's Public Assistance program, offers reimbursement for critical community functions such as building code administration, code enforcement, floodplain management administration and enforcement, and performing substantial damage inspections in affected communities.

As an aid to community disaster response, the Code Council, in partnership with the National Council of Structural Engineers Associations (NCSEA), sponsors the Disaster Response Alliance (DRA) to help communities begin to recover as quickly as possible following a major disaster. The DRA maintains a single national database of skilled volunteers willing to assist with response and recovery activities. These activities include post-disaster building safety evaluations, rapid and detailed safety assessments, building damage assessments, building inspections, and other code-related functions. Additionally, the DRA maintains a national database of skilled volunteers and makes it available to government agencies at all levels to assist communities in their time of need. The activities of DRA volunteers and other code-related safety programs are eligible for reimbursement under FEMA's post-disaster Building Code and Floodplain Management Administration and Enforcement policy described above.

As communities recover from disasters, building codes and standards are critical to safe, sustainable, and resilient rebuilding and construction. Damage costs from major disasters topped $95 billion in 2020. Adopting the most recent editions of codes and standards and using them as a basis for making informed decisions about rebuilding and making investments in resilient infrastructure following a disaster is time and money well spent.

Karl Fippinger, CEM, PMP, is vice president, Government Relations – Fire and Disaster Mitigation for the International Code Council. He is a Certified Emergency Manager and brings more than 25 years of public and private sector experience in federal, state, and local disaster preparedness, response, recovery, and mitigation. He is a 30-year veteran of the fire and emergency services having served as an assistant fire chief with the Occoquan-Woodbridge-Lorton Volunteer Fire Department in Prince William County, VA as well as an adjunct fire and rescue instructor for the Fairfax County Fire and Rescue Department in Fairfax County, VA.

Dräger

Looking for American-made N95 respirators?

MADE IN ★ USA ★ SINCE SEPTEMBER 8, 2020

With a new plant in the USA, Dräger has you covered

For ground personnel working in dusty environments, respiratory protection is essential. The Dräger X-plore® 1750 N95, our next-generation particulate filtering facepiece respirator, offers distinct improvements in comfort and protection. And it's now made right here in the US.

FOR MORE INFORMATION VISIT WWW.DRAEGER.COM

Dräger. Technology for Life®

Psychological Effects of COVID-19 on Frontline Workers

By Hannah Bennett

The COVID-19 pandemic significantly impacted the lives of healthcare workers and first responders – impacts they are still feeling. As workers on the frontlines, these people took a harder hit than the rest of the American population when COVID-19 swept across the nation. Several studies have shown that the pandemic increased a person's likelihood to have negative impacts on mental health and led to the development of new coping strategies among healthcare workers and first responders.

As the world went into lockdown, healthcare workers and first responders went to work. A heavy burden was placed on these frontline workers, as they had no choice but to put their health and lives at risk to serve their communities. The impact of the pandemic can be seen in many psychological, emotional, and physical effects. The fear of uncertainty with what the pandemic might bring, deaths to come, and extended, isolated quarantines made healthcare workers and first responders highly susceptible to negative consequences in mental health.

Increase in Mental Illness

First responders and healthcare workers are incredibly resilient, but they are not immune to the damaging effects of traumatic events such as the pandemic. According to the National Center for Biotechnology Information (NCBI), frontline workers are at a higher risk of developing mental illnesses.

In fact, 32 scientific studies agreed that the most common psychiatric disorders diagnosed among healthcare workers in severe epidemics are post-trauma stress syndrome (PTSS), depression, and anxiety. Furthermore, female nurses who had close contact with COVID-19 patients were found to have higher levels of stress, depression, and anxiety than their male coworkers.

> ***Frontline workers had increased rates of mental illness during COVID-19. They also often lacked the mental and physical capacity to focus on their own health.***

One of the 32 studies, conducted among Chinese healthcare workers during the COVID-19 outbreak, found that 36.1% exhibited signs of insomnia. Another study examining workers with depression, anxiety, and insomnia deduced that over 70% of them were going through psychological distress. Not only were first responders and healthcare workers experiencing higher rates of mental illness, they were also not getting enough sleep to rest and have the mental and physical capacity to address those issues and pursue their own health.

During the COVID-19 pandemic, healthcare workers also showed signs of somatization, a process of expressing emotional or psychological stress through physical (somatic) symptoms. For many nurses, doctors, and other medical professionals, this looked like headaches, throat pain, and lethargy. One survey found frequent instances of somatization, with 42.7% of frontline nurses identifying somatic symptoms.

All the above findings and more point to a serious decline in the psychological well-being of frontline workers during the pandemic. The immense physical and psychological pressure of working as a nurse, emergency medical technician (EMT), or other frontline professional led many workers during COVID-19 to develop disorders or exacerbate existing mental health concerns.

Factors Contributing to Psychological Distress

There are several factors causing these high rates of mental illness, insomnia, somatization, and other symptoms of psychological stress. Stressors such as fear of the unknown, self-isolation during quarantines, a lack of access to proper equipment or medical materials, and other job-related factors all contributed to the psychological distress that frontline workers felt as they responded to the pandemic.

One of the primary stressors many healthcare workers and first responders experienced was infection-related fears. Reports spanning 17 studies identified fear as the prominent stressor for frontline workers, with the most common fears being: (1) fear of the unknown; (2) fear of becoming infected; and (3) fear of threats to their own mortality. Worried not only for their own health but the health of their loved ones, frontline workers commonly reported fear of bringing the virus to vulnerable family members and colleagues. Many of their loved ones fell victim to the virus, which caused further depression and insomnia.

The social and cultural impact of the pandemic took a further toll on healthcare workers and first responders as they were cut off from all social support – family gatherings, time spent with friends, and any other form of social contact. Loneliness and self-isolation quickly became a prominent issue in regard to the mental and emotional health of frontline workers.

Additionally, family members and friends distanced themselves from healthcare workers and others who may have been directly exposed to the virus, widening the gap between human connections. Lack of social support coupled with insomnia were the top two influences of levels of anxiety, stress, and self-efficacy for frontline workers.

The working conditions under the COVID-19 pandemic proved to have a major impact on the physical and emotional health of frontline workers. As hospitals and clinics were overwhelmed with unprecedented intakes, healthcare workers became exhausted. Long hours, most of the day spent on their feet, and a steady flow of patients made medical centers a stressful place to work for the duration of the pandemic.

In addition to physical stress on the job, healthcare workers also adorned heavy protective gear to protect their health. This was found to add to the distress of working in hospitals and increased the difficulty of performing important procedures. Many healthcare workers also doubted the efficiency of such protective gear, contributing to higher levels of depression, anxiety, and stress than those who believed their gear to be adequate.

Addressing the Psychological Impact of COVID-19 on Frontline Workers

Though there has been a heavy burden placed on frontline workers, much can still be done to improve their health. Learning new coping strategies, opening up about the psychological impact of COVID-19 with other colleagues, eliminating the stigma surrounding issues of mental health among frontline workers, and other strategies can help to alleviate some of the symptoms of psychological distress:

- *Coping strategies* – Healthy coping strategies frontline workers might practice include eating well, exercising, pursuing therapy, and connecting with loved ones like friends and family members.
- *Opening up with colleagues* – Colleagues can speak openly about COVID-19's impact on their health, physically and emotionally, and talk about mutual issues they face.
- *Eliminating the stigma* – To mitigate stigma surrounding issues of mental health, managers and supervisors should lead by example, opening up about their own struggles with mental health in the pandemic and offering tools to frontline workers to work through their mental health concerns.
- *Other strategies* – Access to mental health treatment should be extended to all frontline workers. Healthcare workers and first responders can also practice taking more breaks, taking a day off from work to mentally reset if needed, stepping back from news and other media sources, and checking in with themselves by journaling and monitoring symptoms of mental illness, such as depression.

Experts are still learning about how the pandemic affected frontline workers and are developing new measures to address the psychological effects that many still face today.

Hannah Bennett is a content specialist for AddictionResource.net, an informational content guide that provides resources for individuals who struggle with addiction and their loved ones.

COVID-19: Impact on Financial Fraud

By Michael Breslin

The past 16 months have been challenging. COVID-19 left a trail of destruction and a tremendous loss of life. It has had an impact on almost every aspect of daily life. The economy, supply chains, social norms, schools, and places of worship were all affected. The pandemic also led to increased risk of financial fraud and cybercrime. The nation seems to be turning the corner on the pandemic, and people are gradually setting their sights on returning to a new normal way of life.

The digital systems people utilize to socially interact, conduct their business, purchase goods, and in some cases seek medical help, all face increased risk of falling victim to a COVID-19 motivated criminal scheme of attack. With government agencies and the private sector gradually shifting from maximum telework mandates, people are still spending increased time at home working from remote devices.

Bad actors continue to exploit people's uneasiness and anxiety by sending fictitious emails requesting charitable donations, peddling counterfeit personal protective equipment (PPE), or touting a COVID-19 vaccine.

There has been an onslaught of phishing attempts and emails directing unsuspecting people to malicious websites with suspicious attachments. These attempts could lead to loss of personal information, unauthorized access to company networks, and financial fraud. There is no central repository for COVID-19 related fraud. However, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) is a great mechanism for the public to report internet-related crime.

> ***Over the course of the past few months, the Secret Service has observed a clear evolution of the types of frauds being perpetrated… With workers out of the office, many of the normal oversight mechanisms that have might otherwise have prevented an organization from becoming a victim, such as in-person approval for wire transfers, made organizations especially susceptible to (Business Email Compromises) BECs.***
>
> ***—Michael D'Ambrosio, Assistant Director Office of Investigations United States Secret Service***

The sudden surge in working from home across the nation led to increased personal router attacks where, in addition to identity theft attempts, traffic was redirected to malicious domains in attempts to gain employee credentials. These phishing emails represent an easy and cost-effective way to get into a company's systems. Good cyber hygiene and company insider threat practices are the recommended steps necessary to help reduce this risk.

Methods & Trends

Many of the patterns and trends in identity theft that were prevalent four to five years ago are being deployed once again. As witnessed after the Hurricane Katrina disaster relief in 2005 and the big bank bailout of 2008, criminals acted quickly to fraudulently acquire millions of U.S. dollars, capitalizing on the abundance of available money and lack of controls. Each new crisis creates similar vulnerabilities.

During the height of the COVID-19 pandemic, the previously used methods and techniques were resurrected by fraudsters. One example is the increases in COVID-19 themed phishing and fraud campaigns that leverage the coronavirus crisis and the subsequent stay-at-home restrictions. In his statement before the Senate Judiciary Committee on 9 June 2020, Calvin A. Shivers, assistant director, Criminal Investigative Division FBI, warned of this increase in fraud:

> *As of May 28, 2020, the Internet Crime Complaint Center (IC3) received nearly the same amount of complaints in 2020 (about 320,000) as they had for the entirety of 2019 (about 400,000). Approximately 75% of these complaints are frauds and swindles, presenting a challenge for the FBI's criminal program given the sheer volume of submissions.*

One year later with the FBI's release of its 2020 Internet Crime Report, records indicate the agency received a staggering 791,790 complaints of suspected internet crime, representing ~300,000 more complaints than 2019. Reported financial losses now exceed $4.2 billion. Approximately 28,500 of the complaints submitted to the IC3 in 2020 were related to COVID-19.

Early in the pandemic, the Department of Justice (DOJ) established COVID-19 task forces throughout the country with several other agencies including the Federal Emergency Management Agency, U.S. Department of Health and Human Services, U.S. Small Business Administration (SBA), and the U.S. Treasury. DOJ's efforts were supported and augmented by its state and local law enforcement partners, who allowed the DOJ to get a head start in combatting the inevitable fraud. Initial complaints and arrests regarding price gouging and hoarding of PPE (N95 masks, gloves, etc.), COVID-19 related charity scams, investment frauds, and business email compromise schemes were publicized by the U.S. Attorney's Office, Western District of Pennsylvania.

On 17 May 2021, U.S. Attorney General Merrick B. Garland established a Task Force to coordinate investigative efforts across government aimed at combatting COVID-19 fraud. As of May 2021, the DOJ's efforts have led to the charging of approximately 600 defendants with crimes involving over $600 million in 56 federal districts across the United States.

The common factor and motivation for most financial crimes is simple: greed. Criminals use data created by the explosion of online transactions and mobile devices for nefarious purposes like redirecting tax funds, intercepting social security entitlements, and gaining access to sensitive government information. According to data compiled by the Federal Trade Commission (FTC) there have been more than 580,000 complaints filed by consumers to the FTC reporting over $531 million in financial losses related to COVID-19 related scams.

COVID-19 Related Fraud:

- Unemployment insurance scams
- Small Business Loan scams
- Identity fraud (synthetic, individuals, businesses, email accounts) in submitting applications
- Loan fraud associated with the CARES Act
- Fraudulent loans obtained by new businesses or existing business accounts taken over by fraudsters
- Fraudulent use of the Paycheck Protection Program
- Mortgage scams to include fraudulent refinancing, Home Equity Line of Credit (HELOCs), short sale fraud, and loan modification scams
- Treatment scams
- Supply scams
- Healthcare provider fraud related to in-person and telemedicine healthcare services
- Charity scams
- Phishing scams
- App scams
- Investment scams
- Price-gouging scams

All industries have felt the impact of the pandemic as COVID-19 continues to impact the global digital economy, regional economies, industries, businesses, and consumer behavior. Compared to the previous six months, the January-June 2020 LexisNexis Cybercrime Report showed a 38% and 32% growth in bot attacks on financial services and e-commerce merchants, respectively. This demonstrates the extent of fraud with online payment transactions as seen by the onslaught of fraud attempts targeting the Small Business Administration's Paycheck Protection Program. With the Pandemic Unemployment Assistance (PUA) program, an estimated 10% were reported as improper payments due to fraud.

The flood gates appear to be open given the seemingly low barriers to entry. Criminals either are just brazen or believe that agencies cannot handle the number of claims, thereby resulting in many cases of obvious fraud attempts. For instance, criminals have attempted the following tactics: use of deceased identities, use of the same physical address, use of vacant addresses, or houses for sale as an applicant's input address on loan applications are obvious indicators of fraud. Although the use of different types of disposable domains is not a new fraud tactic, there has been an increase in the use of multiple instances of foreign disposable domains.

Resilience of Fraudsters

Crime is certainly not new nor is the ingenuity and tenacity of criminals to find new and creative ways to further their illicit activities. The technology and communication systems

meant to foster good governance and provide for the well-being of civil societies are by default the very systems exploited by criminal actors to commit financial fraud around the world. Financial and cybercrime have no borders.

The COVID-19 pandemic and efforts to provide financial relief to individuals, families, and small businesses had an unintended consequence – it also brought transnational crime into homes. Government agencies at all levels – including law enforcement – are on the front line when it comes to this type of fraud activity. Unemployment fraud, identity theft, money laundering, and other scams have a common COVID narrative. There is no shortage of fraud opportunities with the focus of attack being the Coronavirus Aid Relief, and Economic Security (CARES) Act, Economic Injury Disaster Loan (EIDL), Economic Impact Payment (EIP), and Paycheck Protection Program (PPP).

The SBA dispensed two sources of funding to small businesses negatively impacted by the pandemic: PPP and the EIDL. The issuance of any such government-wide stimulus package is followed by fraud. The United States Secret Service alerted members of the Senate Committee on the Judiciary to the alarming fact that, even assuming "very low rate of fraud, of just 1%, we should still expect more than $30 billion will end up in the hands of criminals."

Well over a year after the onset of the pandemic and subsequent related fraud, the financial losses reported by various law enforcement agencies is staggering. On 12 May 2021, the United States Secret Service reported the seizure of over $640 million in fraudulently obtained funds and effected the return of approximately $2 billion to state unemployment insurance programs. Well-organized fraud rings successfully exploited the COVID-19 crisis to commit large-scale fraud. Statewide government unemployment insurance scams are rampant, resulting in tremendous financial loss to the taxpayer.

The Internet Threat Landscape

The world and its interactions are interconnected and increasingly reliant on the dependability and convenience of technology. Inadvertently, the world's adoption of digital technologies for the ease of business and communications has led the Internet (an open-source medium) to become a nearly limitless reservoir of publicly accessible information. This information, or as commonly referred to as "open-source information" represents a potential treasure trove to criminal actors. Just about anything can be in online open sources including social media profiles, web pages, online newspapers and publications, books, geolocation data, IP addresses, and personally identifiable information (e.g., full names, addresses, social


©iStock.com/Julia_Sudnitskaya

security numbers, dates of birth, metadata, device information, demographic data, and physical traits). This information is often exploited by malicious actors.

As the world struggled with COVID-19, cybercrime increased by more than 600%. A prediction made by Juniper Research in 2018 indicated that by 2023 approximately 33 billion digital records will have been stolen by malicious threat actors.

- In 2020, approximately 11.7 billion devices are connected to the Internet worldwide and are exposed to malicious cyberattacks. Although estimates vary, the number of Internet-connected devices are expected to be as high as 30.9 billion or more by 2025.
- Although third-party quantitative studies were not obtained on the prevalence of specific internet threats such as doxxing (i.e., revealing personal information about someone online without their consent) as of 2020, an analysis of open-source data revealed a drastic increase in the use of doxxing as a tool of political intimidation and personal grievances.
- Nearly 98% of cybercrime incidents make use of social engineering tactics. Social engineering refers to the deliberate use of manipulation or deceitful tactics by a malicious attacker to entice a person to disclose sensitive or personal information.
- According to Verizon Wireless, in 2021:
  - Cyberattackers increased malware attacks against U.S. victims, healthcare, and public sector.
  - Credential theft and social attacks were the cause for 67% of cyber breaches and the majority (86% of breaches) continue to be financially motivated.

On the Horizon – Front-End Identity Authentication & Private Sector Capabilities

The pandemic's impact seems to have strained law enforcement's resources and ability to identify and mitigate this criminal activity. Private sector partnerships are vital to this effort as the vulnerabilities to the nation's financial sector and supply chains have been targeted by fraudsters and cybercriminals.

Supply chain risk management vetting is vitally important as the pandemic exposed the vulnerability of government procurement offices, which often lack expertise to identify threats and conduct proper risk assessments. This is normally the jurisdiction of an organization's investigative teams. COVID-19 exposed the dire need for government to grow these capabilities and seek solutions to better protect their supply chains and avoid rampant fraud and insider threats.

The public sector should implement more rigorous standards and anti-fraud safeguards to better assume a more proactive stance in identifying fraud before it happens. Efforts to improve front-end identity verification and authentication would save taxpayers untold billions of dollars that otherwise would go into the pockets of fraudsters or their bank accounts and crypto wallets.

Business and identity data are not static. They evolve, and connections of risk tend to hide behind them. Businesses are purchased, there are shell and shelf companies, company officers change, and so on. A multi-layered approach is needed that solves the scope of issues around verification, fraud analytics, authentication, and identity proofing without creating a negative experience for end users. Front-end identity authentication is central to how the government dispenses entitlements, stimulus, benefits, and contracts to all types of applicants, including businesses.

The 2020 Internet Crime Report indicated the FBI received a staggering 791,790 complaints of suspected internet crime, representing ~300,000 more complaints than 2019.

Front-end identity authentication also ensures that a person's claimed identity matches their digital footprint, internet behavior, and patterns of activity of a connecting device. New ways are needed to look at digital identities and known patterns of behavior versus that of a bot. Using big data across a shared global network can identify high-risk users accessing systems by looking at behavior that deviates from the norm or from trusted digital identities seen through millions of other consumer interactions.

Digital intelligence can automatically alert information technology professionals to potential threats at the time a user connects to an agency's protected infrastructure. Front-end identity and authentication help protect all types of government portal or network access for citizens, applicants, and employees. This method avoids a futile pay and chase fraud scenario.

Clean-Up the Fraud & Return to Core Mission

Government agencies and their employees are mission-focused and under considerable demands and constraints. The pandemic created broader issues than just individual identity fraud. Businesses are now a big part of the identity verification problem. It is important to keep in mind that companies do not commit fraud, people do. Now is the time for agencies to prevent procurement fraud, supply chain risk, and business compliance schemes by vetting the company on the front-end. Just like individuals, businesses leave many "data footprints" through actions, such as securing assets, establishing points of contact, paying taxes, and legal proceedings. Reliable business intelligence is a must for agencies to be prepared for this type of fraud and to fix vulnerabilities before they happen. Criminals only need to be lucky once, businesses and people must protect the data 100% of the time.

Michael Breslin has more than two decades of experience in federal law enforcement and transnational financial and cybercrime investigations. He serves on the Cyber Investigations Advisory Board of the U.S Secret Service and is the strategic client relations director for federal law enforcement at LexisNexis Risk Solutions. Prior to joining LexisNexis Risk Solutions, he served as deputy assistant director for the Office of Investigations for the Secret Service, where he oversaw the planning and coordination of investigative responsibilities. He serves on the Preparedness Leadership Council and is a board member for the National Center for Missing and Exploited Children.

TELEDYNE
FLIR
Everywhereyoulook™

WE'VE GOT YOUR BACK. LITERALLY.

high sensitivity detection is now able to fit in a simple backpack.

The identiFINDER R700 Backpack Radiation Detector (BRD) offers a hands-free capability for broad-area radiological search and monitoring missions. The identiFINDER R700 provides the user all that is required to successfully perform wide-area searches quickly, efficiently and confidently. Providing the ultimate versatility, the identiFINDER R700 can be placed for stationary monitoring at makeshift checkpoints, fence-line monitoring, and other temporary screening locations. When coupled with radiation monitoring software, the identiFINDER R700 can be used as a fixed-site monitoring tool.

LEARN MORE AT FLIR.COM/R700