RISK MANAGEMENT

Enemy of the State: Ransomware Targets Cities

The Latest Technology to Migitate Property Risks

Five Key Steps in Crisis Management Planning

December 2019

YEAR IN RISK 2019

Looking Back, Moving Forward

RMmagazine.com

WE WANT YOU

Share your expertise and perspective with your peers and help create a stronger and more vibrant risk management community by contributing to *Risk Management*.

Visit **RMmagazine.com/contribute** for details on how you can get involved.

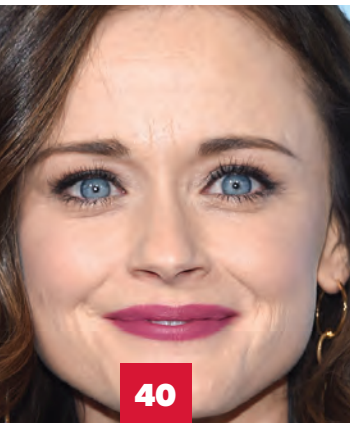
RISK MANAGEMENT

Volume 66, Issue 11

contents

COVER: SHUTTERSTOCK/PHAT1978; THIS PAGE: GETTY/TOM WILLIAMS
NEXT PAGE: TOP PHOTO: ADOBESTOCK/KINWUN; BOTTOM PHOTO: SHUTTERSTOCK/DFREE

FOREFRONT



DETAILS

RISK MANAGEMENT

Editor in Chief
Morgan O'Rourke

Senior Editor
Hilary Tuttle

Associate Editor
Adam Jacobson

Art & Production Manager
Andrew Bass, Jr.

ADVERTISING

Account Executives
Ted Donovan, *tdonovan@RIMS.org*
T: (212) 655-5917

George Schwimmer, *gschwimmer@RIMS.org*
T: (212) 655-6033

CIRCULATION

Quality Circulation Services
Carole Ireland, *carole@qcs1989.com*
T: (413) 442-7300 **F:** (413) 442-7333

Risk Management
P.O. Box 3, Congers, NY 10920
Customer Service: (866) 512-3111
Local: (845) 267-3004
Fax: (845) 267-3478

Member of BPA WORLDWIDE

RIMS

The Risk and Insurance Management Society, Inc. (RIMS) is a not-for-profit organization dedicated to advancing the theory and practice of risk management.

CONTACT US

All submissions and letters should be sent to:

Morgan O'Rourke
Editor in Chief
Risk Management
1407 Broadway
29th Floor
New York, NY 10018
morourke@RIMS.org
T: 212.655.5922
F: 212.655.2694

www.RMmagazine.com

Risk Management Magazine (ISSN 0035-5593) is published 11 times per year, with combined issues in Jan/Feb and July/Aug, and a special issue in April, by the **Risk and Insurance Management Society, Inc.** Offices at 1407 Broadway, 29th Floor, New York, NY 10018; (212) 286-9364; Fax (212) 922-0716. Volume 66, Issue 11.

Subscription rates for **RIMS** members: $80. Non-members: $120. Periodicals postage paid in New York and additional mailing locations. POSTMASTER send change of address notices to *Risk Management Magazine,* P.O. Box 3, Congers, NY 10920.

AN AWARD-WINNING PUBLICATION

AZBEE AWARDS WINNER · EXCEL AWARDS WINNER · FOLIO: EDDIES WINNER · GD:USA AWARDS WINNER

The Climate Risk Tipping Point

Morgan O'Rourke, **Editor In Chief**

In their recent *Future Risks Report*, AXA and Eurasia Group asked risk experts what risks they think will have the greatest impact on society in the coming decade. Perhaps not surprisingly, the number-one risk cited was climate change, particularly as it relates to increased exposure to extreme weather events like floods, storms and rising sea levels. Earlier in the year, the World Economic Forum's *Global Risk Report* similarly listed extreme weather events and the failure of climate-change mitigation and adaptation among the top three global risks in terms of both likelihood and impact.

Given the wide range of extreme weather events this year, it seems these fears are well founded. Some of the strongest hurricanes, cyclones and typhoons on record have caused billions of dollars in damages and claimed hundreds or even thousands of lives. Catastrophic flooding in the Midwestern United States, India and China devastated communities, while conversely, water shortages left others in crisis. Summer heatwaves scorched Europe and India, and wildfires raged in the United States and Australia. The list goes on.

Through it all, the scientific consensus continues to be that governments and businesses need to take steps to prevent climate conditions from getting worse. While this often takes the form of pacts like the Paris Agreement, in extreme situations like in Indonesia and Thailand, governments have considered drastic actions like moving entire cities out of harm's way. Meanwhile, businesses are examining their practices as they relate to climate issues. Indeed, some in the insurance industry are even ending their investment in fossil fuels like coal altogether.

Nevertheless, much more needs to be done and the public has grown increasingly frustrated at the lack of coordinated action from their leaders to forestall climate change's effects. As a result, climate strikes by students, walkouts by tech workers, and climate-related lawsuits against governments and businesses have become more pervasive—so much so that the Collins Dictionary even named "climate strike" its word of the year.

Risk managers need to focus on a wide range of threats, but given climate change's impact, we may have finally reached a tipping point where addressing this risk must be a top priority. ■

ADVERTISERS INDEX

INSIDE

The Latest Technology to Mitigate Property Risks

by Andrew Singer

For years, organizations have employed remote sensing technologies that obtain information about objects or areas from a distance—typically from aircraft or satellites—to assess impacts from natural disasters like hurricanes. But today, thanks to a convergence of factors, including a dramatic drop in remote sensing costs, greater availability of more detailed and abundant data, and advances in artificial intelligence, the technology is increasingly being used to mitigate property risks.

"A new generation of remote sensing technology offers more frequent and less expensive data collection that uses lightweight drone aircraft and satellites," according to a recent BCC Research report. "Built from off-the-shelf parts and delivered to orbit by commercial rocket companies, these technologies are lowering the cost of remote sensing from $10 per square centimeter to pennies."

In some cases, this data is even available to the public at little or no cost. For example, data from the European Union's Sentinel-1 satellites can be accessed for free every six days. Imagery is also available from the National Oceanic and Atmospheric Administration (NOAA), the Civil Air Patrol and other agencies.

Drones are a big reason for the decrease in cost. "One of the most valuable forms of airborne remote sensing, LIDAR imaging, can be performed for $50 a square meter [using drones],

ADOBE STOCK/KINWUM

Want to learn more about risk management? Listen to experienced professionals.

RIMScast is the Society's weekly podcast, providing insight from the risk management industry's leaders and rising stars. Through our in-depth interviews, you will gain valuable insight on the issues that risk professionals face today – from cybersecurity and risktech to reputation and risk culture.

Guests include:

Risk Culture in India

Harshit Baxi
Global Head of Internal Audit and Risk Management
First Source

The Risk Tech Space

Audrey Rampinell
Chief Executive Office and Co-Founder
OnRamp Risk

Virtual Currencies, Blockchain Technology, and the FinTech Industry

Luke Wilson
Vice President of Intelligence
4iQ

The State of Cybersecurity and 5G Technology

Jason Ruger
Chief Information Security Officer
Lenovo

Ruby Zefo
Chief Privacy Officer
Uber

Chris Novak
Global Director
Threat Research Advisory Center
Verizon

RIMS the risk management society

www.RIMS.org/RIMScast

about one-ninth the price of acquiring the same data with a small manned aircraft," BCC Research noted.

In addition to dropping costs, the capabilities of remote sensing technology have never been greater. Thousands, or even millions of images of a building complex or work site can be captured by high-resolution cameras mounted on drones or satellites and interpreted using computer vision technology, 3D reconstruction and deep learning in a way that "completely changes the paradigm of risk management," said Siddhartha Dalal, professor of professional practice in applied analytics at Columbia University's School of Professional Studies.

AI and machine learning are a critical part of the process because human beings simply cannot pore through the sheer number of images being generated. Instead, computers can quickly cycle through the images and learn to identify components. If you want to mitigate risk at a construction site, for example, you need enough images to train the model so it can determine the difference between a ladder or a trench, or whether a worker is wearing a hard hat. If something seems amiss, the system can quickly issue an alert.

The new technologies also offer greater breadth when assessing property risk. Sheri Wilson, national property claims director at Lockton, pointed out that organizations will now have a visual not just of their property, but of their neighbor's as well. This can allow an organization to determine if its neighbor has debris on the ground that presents a fire hazard or is doing construction that could impact adjacent properties.

Because of the technology's promise, the global remote sensing market is expected to increase at a compound annual growth rate of 10.7%, from $10.1 billion in 2017 to $18.9 billion in 2023, BCC Research reported.

NEW APPLICATIONS AND CHALLENGES

The risk management toolkit is evolving, said Beverley Adams, head of visual intelligence services at Marsh. In the past, if you had a risk, you entered it on a spreadsheet and included lots of details. Today, a risk manager still has that spreadsheet, but also attaches a portfolio of images. Some companies are requiring imagery before taking on a property risk, she added. Most companies still require boots on the ground for risk mitigation, but now they have a visual toolkit too.

The global remote sensing market is expected to grow at a compound annual growth rate of 10.7%, from $10.1 billion in 2017 to $18.9 billion in 2023.

Dalal believes that a new business model is developing, in which "infrastructure companies" take pictures and process algorithms for insurers and property owners, reducing the need for field inspectors. These infrastructure firms can then employ these algorithms at multiple companies. "It changes the whole paradigm," he said. "The way we do business will change."

Take roofs, a key weak point in any building because of potential water intrusion. Historically, insurers looked at a roof's age as an indication of its condition, but in reality, "people just don't know," said David Lyman, CEO of Betterview, a company that provides property risk data to insurers. An older roof can have many useful years ahead of it, while a relatively new roof may already be damaged and susceptible to collapse during the next severe weather event. Roofs remain a challenge for field inspectors because of their relative inaccessibility. But with satellite imagery purchased from a commercial vendor and machine-learning algorithms to read and interpret that roof imagery, a firm can pull an image, interpret it and score it. Its condition can be determined remotely and any damage repaired before a hurricane hits, for example, potentially helping it to withstand the storm.

Satellite, aerial (fixed wing aircraft) and drone imagery can be purchased from commercial vendors, and each has their uses. Commercial satellites cover the most territory and they are well suited for hard-to-reach places, like remote islands, but resolution is presently only about 30 centimeters per pixel. Fixed-wing aircraft cover less area, but have higher resolution—five to 10 centimeters per pixel—and oblique views (not just straight down

ADOBESTOCK/KINWUN

like satellites). Drones offer a high level of detail—two or three centimeters per pixel, and even better if you fly close—but their range is limited.

This means that if you want to see whether vegetation like underbrush or trees is encroaching on a building or structure and increasing potential wildfire hazard, satellite imagery may be sufficient. If you want to monitor building construction, fixed wing aircraft might work well. And if you need to assess a roof's condition, drones can provide a level of detail down to the individual screw, bolt or roof fastener.

Technical challenges remain,

however. "If this is a 100-meter race, we are just out of the starting blocks in terms of using visual intelligence for property risk mitigation," Adams said. For example, a group of civil engineers from the U.K.'s University of Birmingham found that detecting cracked railroad tracks is almost impossible using satellite imagery. In a paper published in the journal *IOP Conference Series: Materials Science and Engineering*, they demonstrated that satellite imagery can pick up some larger-scale failures like the washout of a trackbed in a storm, but many train derailments are the result of component failure, and computers need to be trained to recognize individual railway components if remote imagery is to be useful. This can require hundreds of thousands of labeled images for each item, like the switch blades that enable trains to switch tracks. "Determining whether a pair of switch blades is well-positioned through RSIs [remote sensing images] by satellite could be considered," the authors noted. "However, the appropriate algorithm needs to be used for every moment of operation. This seems to not be feasible for many reasons, such as changes in weather conditions and positioning of satellites, which means failure observations through RSIs by satellites offer a limited contribution to inspection."

The authors acknowledge that satellite imagery is becoming common in civil engineering projects, such as bridges, canals, dams and power plants, and is likely to improve. As a result, they suggest some intermediate uses might soon be feasible, like flagging failures "less easily detectable than earthworks, such as track irregularities like buckling." The paper concludes with a caveat, however: "Although such systems are useful for mitigating risk from projects, their productiveness is arguable and operational risk after application is open to discussion."

Other challenges must also be considered. For example, once deployed, how well will the software perform? Will the algorithms generate a raft of false positives and undermine trust in the process? And, if and when a warning flashes across the computer screen, will employees or government officials actually follow through and mitigate the hazard? "It's one thing to identify a risk," Dalal said, "but whether alerts are acted upon is up to human beings." ■

Andrew Singer is a freelance writer based in New York.

Pre-Litigation Incident Investigation Strategies

by Drew C. Timmons

Every insurance policy contains a condition requiring the policyholder to give "prompt notice" (or similar language) to the carrier regarding any potential covered loss. Therefore, when even the smallest incident occurs at a business or involves employees or vehicles, it should be common practice for risk managers to report it to their liability or workers compensation carrier. Even if there is only slight damage to the vehicles, the injury is not reported at the scene or seems relatively minor, or the injured party says they are fine and do not need medical treatment, the risk of a denial of coverage is too great not to provide notice to the insurance carrier. In some circumstances, it might be sufficient to merely notify the carrier and move on. But businesses can take several other small steps that can pay dividends if a possible claim evolves into an extended lawsuit.

Instead of simply passing along notice to your insurance carrier, the better practice is to recognize that an incident could become a lawsuit filed years later, when much of the evidence is gone. That evidence could have alerted you to the nature of the risk, altered your defense strategy, proven the claim was frivolous from the start or saved you from a spoliation sanction. In the current litigious and plaintiff-friendly climate, businesses can gain a much-needed advantage by making a conscious effort to investigate the facts early, preserve all available evidence and evaluate exposure at the onset.

ADOBE STOCK/INTARARIT

INVESTIGATING THE INCIDENT

Following an incident that results in bodily injury or that could lead to litigation, both small and large companies tend to complete a fairly simple incident report that lists basic information like the parties involved and the nature of the incident. As a general rule, and when done correctly, preparing an incident report is recommended for several reasons. First, it provides a reference point of general information regarding the incident and forces the company to take affirmative action to complete it. The report should not only identify the parties involved, but also any witnesses who may be able to provide additional information. Second, an internal incident report should contain a description of the event while it is still fresh in the minds of all parties and before it can be influenced by zealous attorneys. Finally, creating an incident report is evidence of the company's effort to document and/or investigate the incident and take corrective action, if appropriate.

Yet some companies still resist creating these internal reports for fear that it will be discoverable. Indeed, the broad scope of civil discovery in most states is likely to require disclosure of the inci-

dent report, especially if it is company practice to prepare a report in response to every incident. But while discoverability should not be a deterrent from preparing the report, it should be considered when determining what information to include. To that end, do not include sections in an incident report relating to "fault" or "cause." Instead, focus on the facts surrounding the incident. Internal decisions regarding fault or discipline should be made separately and not as a result of a cursory review of the first available facts. Additionally, avoid including instructions in an incident report such as: "don't admit liability," "don't apologize" or "don't offer to pay any money." These instructions will certainly be used against the company in any future lawsuit.

Early investigation benefits the defense as much as, if not more than, a claimant. For one, the more information a company has before the formal discovery process, the better positioned it will be to effectively evaluate the claim before the company is knee-deep in document requests from the claimant's attorney. Completing an incident report is just a small piece of the investigation. It is strongly encouraged that company employees take photographs following an incident as a picture revealing lighting, facial expressions, skid marks and/or scene placement is invaluable. Moreover, although often handled by an insurance carrier, it is advisable to contact any witnesses to obtain written or recorded statements in the hours or days following the incident, not years later when the suit is filed. A witness is much more likely to appreciate your inquiry, rather than be frustrated by it, if the contact occurs closer in time to the incident when memories are fresh. Even unsworn witness statements can be used effectively in civil litigation to establish facts that may later be forgotten.

Do not assume the facts have been established simply because law enforcement investigated the incident and reached its own conclusions. In auto/truck accident cases, investigating officers do not always fully investigate the scene and consider all potential causes, and the statements they receive are usually conflicting. Similarly, in work-related incidents, a purported Occupational Safety and Health Administration (OSHA) violation may not even relate to the actual incident. Retaining experts early in the process can be extremely helpful to establish a true root cause.

Another valuable component of early investigation is assessing your own employees involved in the claim. Companies too often take at face value the version of events provided by employees, while carefully analyzing recorded statements from the claimant for inconsistencies. Instead, take a recorded statement from your employee and compare it to other evidence. Better yet, perform a complete evaluation of your employee as a potential witness—not based solely on how you view him or her, but from the perspective of a juror in a future courtroom. If a suit is filed, this person will be the claimant's counsel's first target and will be seen as your company's representative. Will this person be effective and credible?

It is possible all these investigative efforts will still result in the discovery of unfavorable evidence that must be turned over to the claimant if they file a suit. However, by developing such evidence early, your company may be in a position to resolve the claim without such disclosure and before a lawsuit is ever filed, versus years of expensive discovery, an eventual determination of liability for the company and the claimant refusing to accept a reasonable settlement.

PRESERVING EVIDENCE

Along with your internal fact-finding and investigation of an incident, preserving evidence should be a primary focus. Trial courts can govern the behavior of litigants even before a suit is filed by imposing sanctions for pre-suit failure to preserve relevant evidence (spoliation). To be clear, spoliation sanctions are not only appropriate when a party has intentionally destroyed relevant evidence, but also when such evidence is merely lost, re-used or unavailable. Businesses must make a conscious effort to collect and keep all manner of evidence for future litigation to protect against spoliation sanctions.

Preparing an incident report and creating a specific file relating to a claim, including photographs and statements, is a starting point for preserving evidence, but is not sufficient on its own. In addition, consider preserving other useful evidence: vehicle electronic control modules, email accounts, phone records (including texts), maintenance records, construction designs/plans, hours-of-service logbooks, lockout/tag-out logbooks, video surveillance, training sign-in sheets and disciplinary records. In the normal course of business, many materials are erased, reused or thrown away without a second thought. These may not have even contained facts harmful or helpful to either side, but a claimant's seasoned litigator can take advantage of the absence of any arguably relevant evidence, and the consequences can include an adverse inference to the jury regarding the content, the exclusion of testimony and/or the striking of defenses or pleadings.

During your pre-suit investigation, in cooperation with your attorney and insurer, attempt to identify and preserve all papers, tangible evidence and electronic data possibly containing information pertinent to your subject incident, the claimant and any involved employees or company property. Moreover, if you receive pre-suit correspondence from an attorney or claimant identifying specific evidence to preserve, you must take affirmative action to keep whatever is identified and remains available. ■

Drew C. Timmons is a partner at Swift, Currie, McGhee & Hiers, LLP.

Managing IIoT Product Defect Risks

by Jude DiBattista

The industrial internet of things (IIoT) is reinventing manufacturing as a highly connected enterprise dependent on machine-produced data flowing from equipment on the factory floor and disparate locations over high-bandwidth wireless and wired networks to IT data centers and control systems in the cloud. The IIoT offers great opportunities for manufacturers to increase efficiency, reduce costs and make products that align more closely with buyers' demands. However, the downside is elevated cyberattack risks.

Manufacturing data presents hackers with a host of attractive opportunities from stealing intellectual property like blueprints and schematics to shutting down a production line until a ransom is paid to corrupting a product's specifications, which can cause a catastrophic product liability claim.

The information transmitted within industrial control system networks has been vulnerable for decades as the internet has evolved. IIoT has vastly expanded the number of access points due to the greater use of wireless networks, the proliferation of sensors because of lower costs, and reliance on cloud computing. Once a hacker finds a way to penetrate a system, they can move into and through the network, until they arrive at the goldmine—the operating systems that control the factory equipment. This is unfortunately becoming increasingly common.

A March 2019 study by Kaspersky Lab found an alarming increase in the number of cyberattacks targeting industrial control systems. By and large, these incidents are intentional, meaning that the hackers have very specific aims for perpetrating the attacks. According to Verizon's *2018 Data Breach Investigations Report*, 86% of cyberattacks against manufacturers are, in fact, targeted.

Most of these hacks are designed to steal information and then sell it on the dark web; others are intended to disrupt manufacturing operations. Of greater concern is the possibility of a hacker attacking a factory machine producing a component that goes into finished products like vehicles or airplanes. If hackers got inside the machine's operating system, for example, they could alter the component's specifications ever so slightly. To the human eye, it may look perfect, but its composition (the materials making up the component) and/or its dimensions (the size and shape of the component) might be defective and cause a disaster.

A 2017 study of robotic industrial machines by cybersecurity firm Trend Micro indicated a number of problems, including outdated software, inferior software protection and weak network security, increasing the risk of unauthorized access. Researchers easily

ADOBE STOCK/PHONLAMAIPHOTO

Being the #1 cybercrime target is nothing to cheer about.

But, you can cheer about holistic real-time defenses for the most easily hacked entry points to your data — every smartphone, tablet, laptop, desktop, and IoT device you use to do business.

MCPc's unique Chain-of-Custody Security Solution℠ delivers SecurityCertainty℠ to protect your data, manage the complexity and sustainability of technology, ensure consistency in security, and ultimately, mitigate business risk.

To learn more, please contact
Andy Jones, CEO | andyjones@mcpc.com

Achieve **SecurityCertainty**℠

MCPc THE DATA PROTECTION COMPANY

The United States is the #1 target for targeted attacks at 38% and will account for half of breached data by 2023.
https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html

hacked one machine's network to alter the robot's movements by two millimeters, introducing minor defects into the manufactured product.

Not only are planes and vehicles susceptible to the risk of hacker-engineered defects, any product made to incorrect engineering specifications is at risk of failing. For example, the chemical formulas in pharmaceuticals, pesticides and even household goods can be altered to increase the risk of injury and illness.

Harmed individuals may bring lawsuits against the company that produced the defective component, the equipment manufacturer that embedded the component in the final product, and the software vendor of the IIoT operating system. The company could face serious loss from having to recall products and cease production until it discovered and fixed the problem. Individual directors and officers might also be held liable if proper governance is found lacking. Cases may drag on for years, undermining the reputation of the defendants while also significantly depleting their bank accounts.

The heightened risk of liability will not slow the pace of IIoT adoption—the IIoT market is expected to generate an annual $85 billion by 2020. Smart machines are regularly touted as one of the major planks in the so-called Fourth Industrial Revolution, the next era of technological advancement. In fact, manufacturers that fail to embrace IIoT may soon be at a competitive disadvantage. According to a 2017 study by Deloitte, a more flexible, adaptive production system is almost imperative for manufacturers that wish to either remain competitive or disrupt their competition.

These new adaptive systems would use internet-enabled sensors that measure temperature, moisture, vibration, density, weight, speed and other factors, depending on product manufacturing details. When analyzed, this information could indicate machine wear and tear and variances in tolerance and tooling drift, guiding more timely maintenance and repair, as well as more efficiently controlling production workflows.

When data from all the factory equipment is connected in the cloud and analyzed, a manufacturer could speed up or slow down production velocity. Benefits would include lower machine utilization, reduced inventory costs, and increased customer satisfaction. The primary benefit, of course, would be higher product quality.

Given this value, the onus is on manufacturers to manage the escalating risks of a cyberattack and resulting product defects. Best practices would include routine upgrades and patching, state-of-the-art firewalls and intrusion detection software, data segmentation protocols, routine penetration testing, as well as mandatory training to help employees spot phishing and other forms of cyberattacks.

Insurers can also help manufacturers via product liability insurance, which would absorb the potentially catastrophic costs of a major product liability suit. Depending on the insurance company, coverages may be expanded to absorb expenses related to product defects and product recalls. Insurers can also provide professional services that extend beyond the assumption of a manufacturer's product-related loss exposures to identify key risks to business models and operations and enhance overall business resilience. ■

Jude DiBattista is senior vice president and underwriting leader of excess and surplus lines at QBE North America.

BE PREPARED FOR ANYTHING

Since 1954, *Risk Management* has provided readers with the latest in risk management news, insight and analysis. Whether it is the fundamentals of insurance and disaster preparedness, dynamic issues of cybersecurity and reputational risk, or anything in between, we give you the information you need to meet the challenges of today's evolving business landscape.

Subscribe to *Risk Management* magazine today.

Visit **RMmagazine.com/subscribe** for more details.

RISK MANAGEMENT

Insurance Considerations for Shooting Incidents

by Robert M. Horkovich and Jorge R. Aviles

Gun violence in America is on the rise. As of November 13, there were 365 reported mass shooting events and 33,944 gun deaths this year in the United States, according to the Gun Violence Archive. Along with the incalculable human suffering left in their wake, shooting events also expose entities of all types and sizes to massive financial liabilities. A September report by the Democratic staff of the U.S. Congress Joint Economic Committee put the total annual cost of gun violence in America at an estimated $229 billion. Given this vulnerability, all entities from school districts and large event venues to small businesses should examine their current insurance programs and study the available options that can provide coverage in the event of a shooting tragedy.

GETTY/MEGAN JELINGER

EXPOSURE TO LOSS AND LIABILITY

Losses and liabilities stemming from a shooting incident can be staggering. These costs include, but are not limited to, business income loss, defense and indemnity costs arising out of victim lawsuits, property repair, and less traditional expenses such as trauma counseling and media consulting.

For example, two years ago, 58 people were killed and hundreds wounded at a Las Vegas music festival in the deadliest mass shooting event in U.S. history. Some of the victims recently agreed to settle their lawsuits against MGM Resorts, the owner of the Mandalay Bay Resort and Casino (from which the shooting originated), for $735 million to $800 million. The final amount will depend, in part, on how many of the 4,440 plaintiffs choose to take part in the settlement. The settlement creates the third-largest victims compensation fund ever, surpassed only by the funds created following the September 11 attacks and the BP oil spill in the Gulf of Mexico. According to MGM Resorts Chairman and CEO Jim Murren, the company's goal was to "resolve these matters so our community and the victims and their families can move forward in the healing process."

The enormous cost of the Las Vegas shooting is not an isolated event. It is estimated that the Orlando Pulse nightclub shooting, in which 49 people were killed, will cost approximately $385 million, excluding the cost of mental health counseling. The 2007 Virginia Tech shooting also led to an estimated $48.2 million in litigation and recovery costs. It cost $50 million to build the new Sandy Hook Elementary School, and Broward County spent more than $1.2 million after the 2017 shooting at Fort Lauderdale-Hollywood International Airport just to reunite travelers with luggage, replace carpet and tiles, and perform a crisis response assessment.

INSURANCE COVERAGE FOR SHOOTING EVENTS

Recently, bus stop ads in Los Angeles have sprung up addressing insurance for shooting events. "If there's a shooting, are you covered?" read one. Another promoted "mass shooting insurance," calling it "America's signature coverage." While these ads were part of a campaign to raise awareness about gun violence and no actual insurance was for sale, the ads do belie a key reality: The threat of gun violence has developed to the point that it is expected that entities can, or should be, insured against it.

Traditional insurance programs potentially cover many costs and liabilities stemming from shooting events. But pitfalls abound, some inherent in policy language, others created by the insurance companies' either narrow or broad interpretations. In general liability policies, for instance, insurance companies may argue that coverage is not triggered unless the policyholder is deemed liable for the event or an employee perpetrated the shooting. Importantly, general liability policies may not provide coverage for crisis management expenses, counseling and funerals. Insurance companies might also assert that standard exclusions, such as for acts of terrorism, preclude coverage and some liability policies even exclude gun-related violence entirely.

As for property insurance, while it should provide coverage for direct damage to facilities, insurance companies may argue that the coverage attached to most property policies does not cover expenses related to having to demolish and then completely rebuild a new venue, as is often the case after a shooting due to the event's emotional impact. In addition, property insurance policies might also tie their business income coverage grants to actual physical property damage. But after a shooting event, while the physical structure itself might have sustained relatively minimal damage, the business might not resume operations for months, if ever.

ACTIVE-SHOOTER INSURANCE

Recognizing these gaps in coverage, policyholders have begun to demand tailored insurance coverage to address the aftermath of a shooting to protect both public and private entities. As reported by the *Wall Street Journal*, school districts are increasingly looking into purchasing active-shooter insurance to protect themselves from the risk.

"It at least gives us some peace of mind that, in the event of horrible tragedy, we can begin to put things in place," said Lance Erlwein, treasurer of Belpre City Schools in Ohio. In July of this year alone, insurance company McGowan Program Administrators sold about 120 active-shooter insurance policies, according to managing director Paul Marshall.

This emerging type of coverage is meant to cover those expenses typically associated with gun violence incidents that may not be covered by other, more traditional insurance offerings. "Many clients like these policies because they offer you crisis management services, medical expense coverage, job retraining and relocation and other supplements you might not have under your other policies," said Tarique Nageer, terrorism placement advisory leader at Marsh. Active-shooter insurance can also provide liability protection when lawsuits arise, as well as coverage for costs related to handling media coverage and public perception, and other emergency response services such as temporary security and setting up a call center. It can also provide coverage for on-site counseling and for the victim's funeral expenses.

As with any other insurance product, however, prospective policyholders should be keenly aware of any exclusions that might limit or preclude coverage. These potential pitfalls include policy terms that seek to cap coverage at a certain number of casualties, restrict coverage to damage caused by specific types of weapons, and broadly define excluded acts of terrorism. Further, coverage limits will vary based on a variety of factors, including the venue, location, and number of employees and visitors.

Nevertheless, as society continues to be plagued by gun violence, all entities should review active-shooter coverage as an option to protect themselves and those affected in the event of a tragedy. ■

Recognizing these gaps in coverage, policyholders have begun to demand tailored insurance coverage to address the aftermath of a shooting.

Robert M. Horkovich is managing partner and shareholder and **Jorge R. Aviles** is an attorney in the New York office of Anderson Kill.

The 5 P's of Creating a Crisis Management Plan

by Jack Quinn, Suzanne Folsom and Robert Garretson

In today's dynamic business environment, one of the few certainties is that organizations of all types and sizes are likely to confront an enterprise-defining crisis at some point. Despite the high probability of this occurrence, such an incident will still come as a shock for some.

A crisis is generally defined as a critical event or point of decision that, if not handled in an appropriate and timely manner, can turn into a catastrophe with the potential to harm people or property, seriously interrupt or completely halt business operations, damage an organization's reputation with stakeholders, adversely affect overall enterprise value, spark employee departures, and/or create new opportunities for competitors.

Accepting the reality that a crisis will occur and rejecting the oft-repeated "we'll handle it when it happens" or "there's nothing we can do now since we don't know enough" is the critical first step in constructing a durable strategic crisis preparation and response protocol.

Organizations that use "peacetime" wisely will be much better positioned to curtail the severity and duration when a threat does materialize. A battle-tested framework for effective crisis preparation and response includes:

Planning and preparation: At the outset, developing a written crisis plan requires a candid assessment—best led by independent experts—of the organization's vulnerabilities. This analysis should consider all possible scenarios, from those perceived as likely to so-called "black swans." The process to identify these risks includes interviews with the organization's executives and operations-level leaders, review of its past crises (and how they were handled) along with peer or industry incidents, and open source research such as sell-side analyst reports, relevant federal and state regulatory filings, and macro-industry analysis.

Next, develop tiered and prioritized threat classifications outlining the ideal response approach and the follow-on tactical implementation appropriate for each tier. This should incorporate agreed-upon criteria including objective metrics such as the number of customers or external parties involved, potential financial impact, feedback/input from regulators, expected duration, and relation to other current high-profile issues. The resulting escalation and de-escalation matrix can accommodate the real-life situations in which most crises occur, especially by incorporating new information that changes the dynamics.

The organization's response should be similarly flexible. Preparing materials mapped to each vulnerability discovered above is also essential. Done outside of the pressure of an evolving crisis, draft-

ADOBE STOCK/ONEINCHPUNCH

ing everything from holding statements to deeply researched FAQs to potential social media communications will enable the organization to customize and, as needed, issue these communications quickly.

People: A small group of senior executives designated as the organization's incident management team will provide the oversight and speed necessary in a crisis. Given the enterprise-wide scope of a potential crisis and the need to draw on a wide breadth of internal and external resources to manage it, the general counsel or the chief risk officer often leads this team on a day-to-day basis. The CEO and, when appropriate, the board of directors ultimately have the final say. The incident management team should comprise a range of members of the organization's senior ranks representing each of its major stakeholders, from investors to employees to the media. Every team member should also have a backup.

Additionally, it is useful to identify a series of subject matter experts to advise the team. For example, in the event of a data breach, outside technology, forensic and potentially legal expertise would be immediately available. It is also important to institute a tested system for internally reporting a potential crisis to the designated crisis responders, as well as a clear pathway for communications and direction from the team to be transmitted and implemented across the organization.

Practice: Organizations are best served when they "pressure test" the crisis plan and protocols through the implementation of crisis response drills or table top exercises that simulate the pace, multiplicity of issues, and potential landmines that require deft navigation. Conducted by outside counselors (who alone know the full parameters and extent of the exercise), the results can be illuminating and provide the foundation for briefings to management and members of the board of directors. It can also be helpful to validate the details and implications of this exercise with a designated member of the crisis team (often the general counsel).

Post-Event Evaluation and Review: Whether a real or simulated crisis, the organization must incorporate lessons learned from any incident and address all demonstrated gaps in the crisis plan. Driving this information into the continuous improvement of the process, planning, and materials will enhance organizational preparation to successfully overcome future challenges.

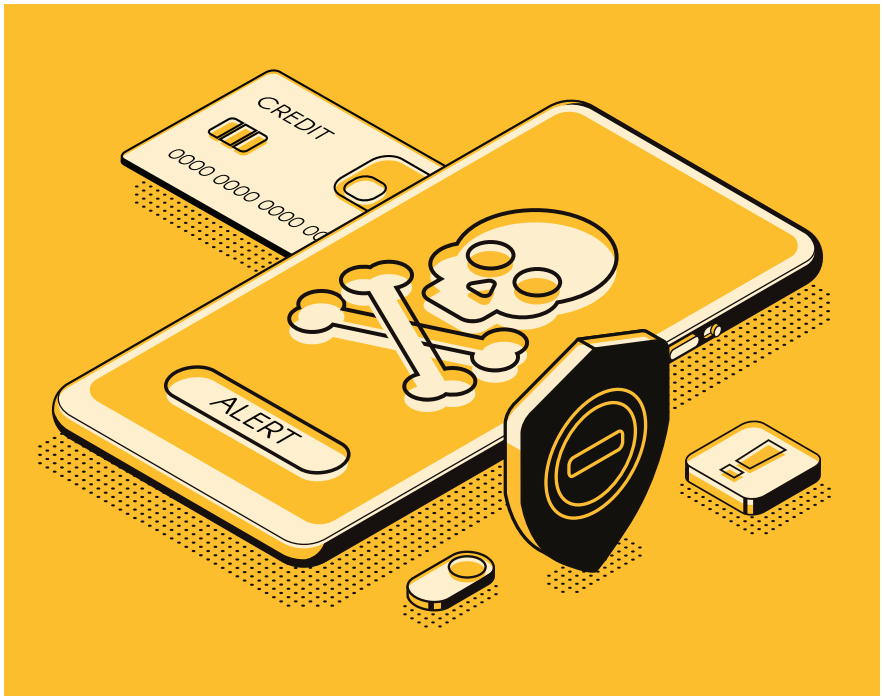
In 2019 and beyond, time is the enemy for any organization in crisis. As response windows continue to shrink, organizations and their leaders are newly empowered through the creation of advanced planning and preparation capabilities to help them thoughtfully protect their people, assets, brands and even their personal reputations. Brands that perform well in trying times can minimize the negative impact, speed their reputational recovery, and stand out from competitors who may not have been as well prepared. ■

Jack Quinn is head of the Manatt, Phelps & Phillips office in Washington, D.C. and chair of the investigations, compliance and strategic response practice. He is a former White House counsel to President Bill Clinton, and co-founder and CEO of crisis communications and public relations firm Quinn Gillespie & Associates. **Suzanne Folsom** is a partner and co-chair of the investigations, compliance and strategic response practice at Manatt, Phelps & Phillips. She is the former general counsel and chief compliance officer at United States Steel and previously played a leadership role in handling crises at AIG, the World Bank, ACADEMI (formerly known as Blackwater), and the Hashemite Kingdom of Jordan. **Robert Garretson** is a managing director in the investigations, compliance and strategic response practice at Manatt, Phelps & Phillips. Previously, he served as the managing director of governance strategy and legal operations at United States Steel.

Combating Mobile Fraud Risk

by D.J. Murphy

Merchants today are increasingly investing in mobile to drive profits. A recent report found that one-third of online merchants expect mobile to represent at least half of total revenue by 2020. As these organizations place bigger bets on mobile, they must understand the risks. Like with any channel, as transactions increase, fraud will grow in tandem because it is easier for fraudsters to hide in greater amounts of traffic. Indeed, mobile fraud attempts grew by nearly 50% since last year. But while merchants recognize the growing threat of mobile fraud, they seem to be complacent regarding their protection capabilities.



Mobile is a particularly appealing target for fraudsters due to the growing number of transactions coming from mobile devices compared to desktops. Criminals are keenly aware that consumers are using their mobile devices more than ever to shop online via mobile browsers, retailer-specific apps or social media commerce. All of these avenues contribute to the heavy mobile traffic patterns that merchants now need to sift through to determine the legitimacy of each transaction.

One of the most common types of fraud is account takeover, wherein fraudsters trick users into downloading a fake app that asks for access to bank accounts and financial information. According to analysts at Javelin, organizations lost $5.1 billion due to account takeover fraud in 2017. Fraudsters also use bots to scale their mobile attacks, such as automated credential stuffing, an attack method that enables bad actors to use username and password combinations stolen in past data breaches to hijack online accounts.

One of the biggest obstacles for merchants is understanding that preventing fraud on mobile requires a different approach than traditional desktop e-commerce. Their processes for spotting fraudulent transactions on desktop (a mix of manual and software systems) might not be able to handle transactions that come through mobile.

In turn, transactions from mobile devices generate much more unique information that can be used to identify and prevent fraud. The systems that merchants have used historically may not be advanced enough to integrate data like information about geolocation, tokenization from payment data, and fingerprint authentication into their fraud decision-making.

Merchants must look at the entry point for e-commerce orders. Did the mobile order come through the desktop website viewed on a mobile device, mobile website, mobile app or social media?

Merchants and fraud experts must also pay close attention to the unique device ID. Device IDs provide valuable informa-

SHUTTERSTOCK/VECTOR POUCH

tion, including the default language on the phone, type of phone and phone carrier. While device IDs can be spoofed, it is uncommon.

They should also track customer behavior closely, as a suspicious change in customer behavior can indicate account takeover. In such cases, especially when authorizing high-value orders, it could be worthwhile for businesses to call the customer directly to verify their identity.

Updating systems to access this information can be expensive, but that cost is becoming a minimum standard for merchants. Once they have information like this, organizations can better authenticate users and assess whether transactions are legitimate. In addition, both failed and successful fraud attempts should be reviewed closely to identify the fraud origin and implement specific security measures.

One of the biggest obstacles for merchants is understanding that preventing fraud on mobile requires a different approach than traditional desktop e-commerce.

PREVENTING MOBILE FRAUD

Because the technology itself is relatively new, mobile is the right place to leverage emerging fraud prevention measures. Several kinds of mobile fraud prevention tools have appeared on the market recently, including:

Multi-factor authentication (MFA): MFA helps prevent fraud by requiring the customer to approve and authenticate any and all transactions. MFA can include biometric authentication techniques such as fingerprints, or more traditional methods like PIN codes, identification questions or text message confirmation. Implementing multiple authentication requirements can decrease the risk of fraud significantly.

Machine learning and artificial intelligence systems: These systems can help merchants not only detect fraud, but also prevent it by predicting emerging fraud threats and trends. For example, artificial intelligence uses historical data (or rules set by the IT team) and real-time behavior intelligence to identify whether transactions are malicious or legitimate.

Behavioral biometrics systems: This technology can identify customers by factors like the way they hold their phone, interact with the screen, or type on the device. It can be effective in catching fraud attempts when the transaction data does not match regular consumer behavior.

Above all, when it comes to mobile fraud prevention, merchants must never assume that the measures they have in place to stop desktop e-commerce fraud will translate to mobile. This new environment requires its own solutions. ■

D.J. Murphy is editor-in-chief of CardNotPresent.com, where he has day-to-day control of the editorial content and oversees programming for CNP Expo, a leading event for the card not present industry.

YEAR IN RISK 2019

–by–
Morgan O'Rourke, Hilary Tuttle & Adam Jacobson

AS THE RISKS BUSINESSES FACE become increasingly interconnected and far-reaching, risk professionals must broaden their perspective on both the traditional and emerging threats that can affect their organization. Whether it is a natural disaster exacerbated by climate change, the latest cyberattack scheme or a new regulatory requirement, risks come from all angles. The following review of some of the most notable risk events of 2019 can help risk professionals be better prepared to meet the challenges ahead.

SHUTTERSTOCK/PHAT1978; JONATHAN WEISS

Copyrights Expire After 20-Year Reprieve

January 1

On January 1, the copyrights expired for tens of thousands of works released in 1923, including classic films, plays, songs and books from the likes of Charlie Chaplin, Cecil B. DeMille, George Gershwin, Louis Armstrong and Agatha Christie. These works are now in the public domain, which means that anyone can broadcast, republish, distribute or remix them without first having to seek permission or pay any royalties to the original rights holder. This was the first set of creative works to enter the public domain since the Copyright Term Extension Act of 1998, which extended the length of a copyright from 75 years to 95 years, or from 50 years after the author's death to 70 years.

Fiat Chrysler Reaches Settlement Over Diesel Emissions Violations

January 10

The U.S. Department of Justice announced that Fiat Chrysler agreed to pay $305 million to settle allegations that it used illegal software on 104,000 diesel-powered Dodge Rams and Jeep Grand Cherokees to cheat on emissions tests in violation of the Clean Air Act, as well as another $6 million for the illegal import of 1,700 noncompliant vehicles. The company also agreed to implement a recall and repair program to fix the affected vehicles, offer extended warranties on the repaired vehicles, and take steps to mitigate excess pollution from them, which could add another $185 million in costs. In addition, Fiat Chrysler will pay $19 million to California to settle similar state regulatory violations. In a separate announcement, the automaker also agreed to pay $280 million to settle a lawsuit brought by vehicle owners.

France Fines Google €50 Million Under GDPR

January 21

France issued the largest GDPR-related fine at the time, levying a €50 million penalty (about $55 million) against Google. According to France's data protection regulator, CNIL, Google was not transparent enough about how user information was collected, stored and disseminated, and failed to obtain proper consent to process user data for ad personalization across its entire range of services. Google

appealed the fine, in part citing concern about the impact on "publishers, original content creators and tech companies in Europe and beyond."

Wynn Resorts Fined $55 Million in Sexual Misconduct Scandal

February 26

The Nevada Gaming Commission fined Wynn Resorts a state record $20 million for failing to report and investigate sexual harassment and assault allegations made by a number of female employees against former CEO Steve Wynn. Similarly, Massachusetts gaming regulators levied a $35 million fine against the company in April for concealing information about sexual harassment allegations during a suitability investigation the state conducted prior to granting a license to build a casino. Current CEO Matthew Maddox was also fined $500,000 for not investigating a misconduct complaint. Wynn Resorts was allowed to retain its casino license in both states. **1**

SEC Names Its First Chief Risk Officer

February 28

The U.S. Securities and Exchange Commission announced that it was appointing Gabriel Benincasa as its first chief risk officer. SEC Chairman Jay Clayton created the position to strengthen the agency's risk management and cybersecurity efforts after the discovery of a 2016 breach in which hackers broke into the agency's EDGAR database and gained access to information about publicly traded companies to use for illegal trading. Benincasa will coordinate the SEC's efforts to identify, monitor and mitigate key risks facing the agency and advise on other matters related to enterprise risks and controls. **2**

Alabama Tornado Kills 23

March 3

A rare EF4 tornado with wind speeds reaching 170 miles per hour touched down in Lee County, Alabama, cutting a mile-wide swath of destruction. By the time it dissipated after travelling some 70 miles, at least 23 people had been killed. It was the deadliest tornado in the United States since 2013, when an EF5 tornado killed 24 in Moore, Oklahoma, and the strongest since 2017, when another EF4 struck Canton, Texas. The tornado was part of a larger outbreak of more than 30 twisters that tore through Alabama, Florida, Georgia and South Carolina during the same weekend, destroying more than 1,000 homes and businesses.

All Boeing 737 MAX Aircraft Grounded After Crashes

March 13

After two crashes killed a total of 346 people in five months, airlines and federal governments around the world grounded all Boeing 737 MAX aircraft. On October 29, 2018, Lion Air flight 610 crashed after takeoff in Jakarta, Indonesia, followed by the March 10, 2019, crash of Ethiopian Airlines Flight 302 just minutes after departure from Addis Ababa, Ethiopia. Investigators believe problems with a newly introduced safety feature called the Maneuvering Characteristics Augmentation System (MCAS) may have caused the accidents. In October, Boeing reported that costs of the continued grounding of the 737 MAX had reached $9.2 billion from lost revenue, compensation to victims' families, and compensation to airlines that have lost business due to cancelled flights and unfilled aircraft orders. Boeing also faces lawsuits from pilots over lost wages. **3**

Southern African Nations Endure Catastrophic Cyclone

March 14

Madagascar, Mozambique, Zimbabwe and Malawi were hit hard by Cyclone Idai, which brought strong winds, heavy rains and flash flooding that affected three million people in the region, causing more than 1,300 deaths and an estimated $2 billion in damage to infrastructure, homes and crops. The storm is the deadliest and costliest ever recorded in the South-West Indian Ocean basin. The lack of clean water in the storm's aftermath also led to a

GETTY/ETHAN MILLER, TOM WILLIAMS; SHUTTERSTOCK/G0D4ATHER

YOU NEED A PARTNER

At WorkPartners, we believe that when things work together, they work better. That's why we offer fully integrated solutions to more efficiently manage the health and productivity of your workforce. The result? Reduced costs, improved employee engagement, and a healthier bottom line. Now that's the power of partnership.

Absence Management

Life Solutions

Workers' Comp

Onsite Services

Analytics

Visit us at **WorkPartners.com**

WorkPartners

cholera outbreak in Mozambique, with more than 6,000 confirmed cases before it was contained in May. Six weeks after Idai made landfall, Mozambique was hit again by Cyclone Kenneth, which caused 52 deaths and another $100 million in damages.

Mosque Shooting Prompts New Zealand Gun Ban

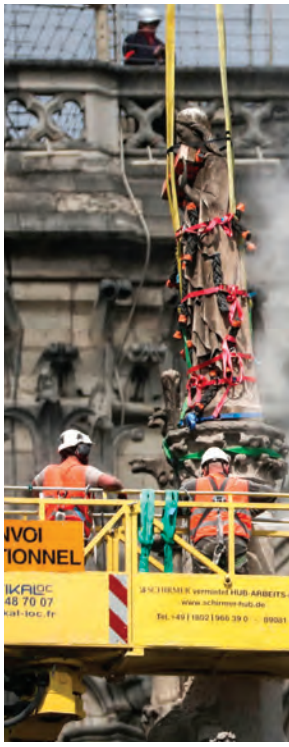
March 15

A terrorist gunman killed 51 people and injured 49 others in two mosque shootings in Christchurch, New Zealand. The shooter reportedly expressed white supremacist, anti-immigrant and anti-Muslim views that authorities believe motivated the attack. Less than a month after the massacre, the New Zealand government passed a law banning most semi-automatic weapons and assault rifles, as well as magazines and any parts that can be used to assemble prohibited weapons. The government also initiated a six-month buy-back program that had collected more than 19,000 guns by mid-September. A royal commission that was convened to investigate how the attack could have been prevented is expected to release its findings next year. **4**

Fisher-Price Recalls Sleepers After Infant Deaths

April 12

Fisher-Price recalled 4.7 million Rock 'n Play Sleepers after a Consumer Reports investigation revealed that the product was tied to at least 32 infant deaths since 2009. According to researchers, the design of inclined sleepers like the Rock 'n Play increases the risk of accidental suffocation and strangulation. Manufacturers Kids II and Dorel Juvenile subsequently issued recalls of similar infant sleeper products as well. In November, the U.S. Consumer Product Safety Commission warned consumers to stop using all infant sleepers—even models that have not been recalled—after connecting as many as 73 infant deaths and 1,100 incidents to the products between January 2005 and June 2019. Fisher-Price and parent company Mattel face multiple lawsuits from victim's families alleging defective design and negligence. **5**



Fire Damages Notre Dame Cathedral

April 15

A fire in the Notre Dame cathedral in Paris caused massive damage to the 700-year old landmark's spire, roof and walls that experts believe could take decades and billions of dollars to repair. While the cause of the fire remains unknown, authorities said there was no evidence that it was set deliberately, instead suspecting it was due to an electrical short, perhaps related to an ongoing renovation project. Months after the fire melted the lead-covered roof, lead concentrations in the surrounding plaza and adjacent roadways remained extremely high, raising concerns about the impact on nearby residents. **6**

550 Workers Die After Indonesian Election

April 17

Following Indonesia's general election, more than 550 election workers and security officers died from fatigue and overwork-related illnesses, including heart attacks, strokes and respiratory failure, while another 4,300 workers fell ill. Considered the most complex single-day election in the world, more than 240,000 candidates vied for 20,000 seats in simultaneous national and regional votes at both the presidential and legislative levels. Seven million workers staffed more than 800,000 polling stations to serve the country's 193 million eligible voters. Indonesian officials are reportedly considering a variety of measures to ease the burden on election workers before the next general elections in 2024, including deploying more medical personnel, separating national and local elections, and adopting electronic voting machines.

Deadly Cyclone Strikes India

May 3

The Category 4 storm Cyclone Fani made landfall near Puri in the Indian state of Odisha, destroying buildings, homes and crops, killing at least 89

GETTY/SANKA VIDANAGAMA, THE WASHINGTON POST, KENZO TRIBOUILLARD, ASIT KUMAR, ANDREW LICHTENSTEIN; SHUTTERSTOCK/JMIKS

people and causing an estimated $8.1 billion in damages throughout eastern India. While it was the deadliest cyclone to strike Odisha in decades, the death toll paled in comparison to a Category 5 cyclone that killed more than 10,000 people there in 1999. Experts attributed the lower casualty numbers to improved disaster preparedness and storm tracking measures, and a concerted effort by government authorities to inform the public about the impending threat by deploying 1,000 emergency workers and 43,000 volunteers, sending some 2.6 million text messages, and broadcasting alerts on television and public address systems. In addition, more than one million people were evacuated in less than 48 hours from the high-risk areas in the storm's path. **7**

Ransomware Wave Crashes U.S. Cities

May 7

The city of Baltimore was the victim of a ransomware attack that forced the shutdown of many online services, resulting in an estimated $18.2 million in lost revenue and system restoration costs after officials refused to pay the 13 bitcoin ransom (then about $76,000). U.S. cities have increasingly been the target of ransomware attacks (see page 30). Cybercriminals also targeted several Florida town governments in May and June, with Lake City paying nearly $460,000 and Riviera Beach paying almost $600,000 to recover their computer and phone systems, while 22 municipalities in Texas fell victim to a coordinated ransomware attack in August. **8**

Indian City Runs Out of Water

June 19

Officials in Chennai, India's sixth-largest city, announced that the city had reached "Day Zero" and was almost entirely out of water after its four main reservoirs dried up. The water crisis forced the city's 10 million residents to rely on dwindling wells, wait in long lines to fill containers from emergency water tankers provided by the government, or purchase water from private companies. While some of Chennai's water woes can be blamed on drier than normal monsoon seasons in 2017 and 2018, poor resource management has also been a factor as the local government struggles to keep pace with the needs of a rapidly developing economy and booming population. According to the World Resources Institute, 44 countries—home to one-third of the world's population—face high levels of water stress, where irrigated agriculture, industries and municipalities withdraw more than 40% of their available supply on average every year.

Insurers Phase Out Coal Investment

July 1

Citing climate change concerns, Chubb became the first major U.S. insurer to announce that it will stop underwriting and investing in businesses that derive more than 30% of their revenue from coal mining or generate more than 30% of their energy production from coal. The company also said it will not underwrite risks related to constructing and operating coal-fired plants (with limited exceptions until 2022). The move followed a similar announcement made by Zurich in June. According to the International Energy Agency, while global coal demand has been decreasing since 2010, it increased in 2017 and 2018. This is largely due to economic growth spurring a higher demand for electricity in India and Southeast Asian countries like Indonesia, Vietnam, the Philippines and Malaysia, where coal is more readily available than other power sources. **9**

Midwestern United States Inundated by Flooding

July 1

Beginning in mid-March and continuing throughout the spring, widespread flooding plagued the Midwestern United States, particularly along the Mississippi, Missouri and Arkansas River basins. By July, at least three people had died as a result of the flooding and states of emergency were declared in more than a dozen states. AccuWeather estimated that damage costs and economic losses could be as high as $12.5 billion, a figure that included "damage to homes, their contents, and cars, business and farm losses—including crops and livestock, contamination of drinking water wells, infrastructure damage, auxiliary business losses and the long-term impact from the flooding, which will likely contribute to, and exacerbate, health issues."

Marriott, British Airways Fined Under GDPR

July 9

U.K. data regulator the Information Commissioner's Office (ICO) announced that it would fine both British Airways and Marriott International for violating the GDPR. British Airways was fined a record-setting £183 million ($237 million) for a breach that exposed almost 500,000 customers' personal data, including names, login information, credit card numbers, travel details and addresses. Meanwhile, Marriott faced a fine of £99 million ($127 million) for a breach that exposed 339 million customer records worldwide, including 30 million in Europe. The fines dwarf previous ICO decisions, including a £500,000 ($644,000) penalty levied last year against Facebook for failing to protect user information in the Cambridge Analytica scandal. That fine, however, was the maximum allowed under the U.K.'s 1998 Data Protection Act, which has since been replaced by the stricter GDPR.

Ebola Epidemic Ravages DRC

July 17

The World Health Organization (WHO) declared the ongoing Ebola outbreak in the Democratic Republic of the Congo to be a Public Health Emergency of International Concern after cases were diagnosed in the border city of Goma. The declaration designates "an extraordinary event which is determined to constitute a public health risk to other states through the international spread of disease and to potentially require a coordinated international response." As of November 13, Ebola has infected almost 3,300 people and killed nearly 2,200 in DRC, according to the WHO. In addition to the human cost, epidemics have serious economic consequences. The World Bank estimated that the 2014-2015 Ebola epidemic cost the first three countries affected—Guinea, Liberia and Sierra Leone—around $2.8 billion in GDP.

FTC Fines Facebook $5 Billion for Privacy Violations

July 24

The U.S. Federal Trade Commission fined Facebook $5 billion for a series of data privacy violations, punctuated by last year's Cambridge Analytica scandal that exposed the personal data of 87 million users, as well as for its failure to comply with a 2011 FTC consent decree in which the company agreed to shore up its privacy practices following previous privacy violations. As part of the settlement, the FTC also required Facebook to revamp its privacy practices by establishing an independent privacy committee, designating compliance officers responsible for privacy issues, conducting privacy reviews of all new products before implementation, and submitting to regular third-party reviews of its privacy program. **10**

Capital One Hack Affects 100 Million

July 30

Capital One revealed that a hacker had gained access to the records of more than 100 million customers in the United States and Canada. The hacker entered the system through a misconfigured firewall and obtained customer information including names, addresses, phone numbers, email addresses, dates of birth and self-reported income from credit card applications, as well as credit scores, credit limits, balances, payment history, transaction data and, in some cases, Social Security and linked bank account numbers. After posting about the theft on a public message board, Paige Thompson, a software engineer formerly employed by Amazon Web Services, was arrested in connection with the breach. Capital One said it expected the incident to cost up to $150 million, mainly for customer notification, credit monitoring, technology costs and legal support.

European Countries Lose Measles Eradication Status

August 29

Albania, the Czech Republic, Greece and the United Kingdom officially lost their measles eradication status, according to the World Health Organization. Worldwide, the first half of the year saw more measles cases than any year since 2006, with 364,808 cases reported to the WHO, compared to 129,239 cases over the same period last year. Measles cases have increased 10-fold in Africa, twofold in Europe, and threefold in the Western Pacific region. While most countries with active outbreaks have low vaccination rates, the WHO noted a troubling rise in countries with high coverage as well, including the United States, which has had the highest number of measles cases in 25 years. Indeed, the United States would have lost its eradication status in October if an outbreak in New York had not been resolved.

Hurricane Dorian Devastates the Bahamas

September 1

Hurricane Dorian became the strongest Atlantic storm on record to make landfall in the Bahamas when it touched down with wind speeds of 185 miles per hour. It killed more than 65 people and caused widespread destruction throughout the Caribbean and United States. RMS estimated insured losses from the Category 5 storm to be between $4 billion and $8.5 billion in the Caribbean and up to $1.5 billion in

SHUTTERSTOCK/KMH PHOTOVIDEO; GETTY/BLOOMBERG, CHIP SOMODEVILLA

the United States, although economic damages could be much higher as many affected areas were not insured. The Bahamas received the brunt of the storm and the northern islands of Abaco and Grand Bahama, in particular, face "generational devastation," according to Bahamian Prime Minister Hubert Minnis. More than 13,000 houses (almost 45% of the homes on Grand Bahama and Abaco) were severely damaged or destroyed.

Purdue Settles Opioid Lawsuits

September 11

Purdue Pharma, manufacturer of the opioid-based painkiller OxyContin, reached a tentative settlement in the lawsuit brought by 23 states and more than 2,000 cities and counties over the company's role in the opioid crisis. Under the deal's conditions, the Sackler family, which owns Purdue, would give up control of the company but admit no wrongdoing, while Purdue would file for bankruptcy and become a trust that solely manufactures drugs to help combat the opioid epidemic. Additionally, the company would pay $10 billion to $12 billion, including $3 billion specifically from the Sacklers. Some of the parties suing may not agree to the settlement and could continue with individual lawsuits, arguing that the settlement would not be enough to make up for the scope of the company's role in the opioid crisis. In March, Purdue settled an opioid lawsuit with the state of Oklahoma for $270 million, while the Sacklers agreed to pay $75 million to fund a national addiction treatment and research center at Oklahoma State University.

Executives Urge Passage of U.S. Gun Control Laws

September 12

Chief executives of 145 companies signed a letter calling gun violence a public health crisis in the United States and asking the Senate to pass "common-sense, bipartisan gun laws." The companies represented span the retail, technology and financial sectors, including Dick's Sporting Goods, Royal Caribbean Cruises, Levi Strauss, Airbnb, Uber, Yelp and Bain Capital. Specifically, the group called for the passage of stronger background check laws and advocated for "red flag laws," which allow family or law enforcement to report warning signs of individuals who may pose risk of harm to themselves or others and temporarily prohibit their access to firearms. In addition, a number of retailers, including Walmart, Walgreens and CVS, began asking customers not to openly carry firearms in their stores, even in states where open carry is permitted. Walmart also announced plans to reduce weapons sales, including ceasing sales of some forms of ammunition and all sales of handguns in Alaska, the last remaining state where it offered them. According to the Gun Violence Archive, there have been 365 mass shootings in the United States (as of November 13), including an August 3 shooting in which 22 people were killed at a Walmart in El Paso, Texas. **11**

PG&E Reaches $11 Billion Wildfire Settlement

September 13

Power utility PG&E, which declared bankruptcy in January because of growing wildfire liability, agreed to pay an $11 billion settlement to insurers for claims paid to businesses and homeowners for damages incurred by wildfires caused by its equipment. In June, the company also paid $1 billion to local governments and state agencies in California for fire damages. More than half of those funds were earmarked for damages from the 2018 Camp Fire, which killed 85 people and destroyed 18,000 homes and businesses, while the rest covered costs from 2015 and 2017 fires. PG&E still faces claims from wildfire victims. In November, the utility said it had incurred an additional $6.3 billion in bankruptcy and wildfire-related costs during the year. That figure could rise, however—while the actual cause has yet to be determined, a PG&E transmission line is suspected to have sparked the Kincade Fire, which burned 78,000 acres in Sonoma County this October. **12**

Thailand, Indonesia Explore Moving Capital Cities

September 30

In an effort to reduce congestion and overcrowding, Prime Minister Prayut Chan-o-cha said he was considering moving Thailand's capital city from Bangkok to a currently undetermined location. The Bangkok metropolitan region is home to more than 14 million

people. One month earlier, Indonesia announced similar plans to move its capital from Jakarta to an as-yet-unnamed city that will be built in the province of Kalimantan on the island of Borneo. The Jakarta metropolitan area has a population of more than 30 million and its residents face not only overcrowding and congestion, but also some of the worst air pollution in the world. Of additional concern is that Jakarta is sinking by as much as seven inches per year due to the ongoing depletion of underground aquifers. Coupled with rising sea levels exacerbated by climate change, this has made the city more vulnerable to flooding and other natural disasters. The Indonesian relocation project is expected to cost $33 billion and construction is scheduled to begin in 2021.

MGM Resorts Settles With Las Vegas Shooting Victims

October 3

Lawyers for victims of the 2017 Las Vegas shooting—which left 58 people dead and hundreds wounded—have reached a settlement with MGM Resorts International for at least $735 million. Depending on the number of people who opt in, the total could reach $800 million. Victims claimed that MGM did nothing to prevent shooter Stephen Paddock from bringing 23 rifles and one handgun into a hotel room at the Mandalay Bay Resort and Casino, from which he opened fire on a country music festival below. MGM reportedly has about $751 million in insurance coverage that will cover all or most of the settlement cost.

California Bans Police Use of Facial Recognition Technology

October 10

California passed a law that bans state and local police from using facial recognition software in body cameras through 2023. Proponents of the ban cited a number of factors, including the prospect of creating a surveillance society and numerous studies that have demonstrated the frequent inaccuracy of facial recognition, especially when identifying women, younger people and people of color. Axon, a supplier of body cameras to law enforcement agencies, has even said that it will not use facial recognition in its products until the accuracy of the technology improves. The law makes California the third U.S. state after Oregon and New Hampshire to ban facial recognition use in police body cameras. Various cities, including San Francisco, have also prohibited city departments from using facial recognition, citing similar concerns about accuracy and surveillance. **13**

Massive Typhoon Strikes Japan

October 12

Typhoon Hagibis became one of the most destructive storms to strike Japan in 60 years, killing at least 95 people and destroying more than 90,000 structures, leading to an estimated $7 billion to $11 billion in insured losses. Many areas experienced record rainfall with some receiving 40% of their annual rainfall in two days. The heavy rains caused more than 140 landslides as levees breached and rivers overflowed. Hagibis came on the heels of Typhoon Faxai, which struck eastern Japan one month earlier. RMS estimated insured losses from property damage and business interruption from Faxai to be in the $5 billion to $9 billion range.

Monsoon Rains, Floods Cause 2,100 Deaths in India

October 25

According to Indian Home Ministry officials, at least 2,155 people were killed and 45 reported missing since June in the heaviest monsoon season in the country in decades. The death toll was highest in the western state of Maharashtra, where 430 people died. Heavy rains, flooding and landslides have affected more than 2.6 million people in 22 states, destroying more than 200,000 houses and thousands of acres of crops. Monsoon season in India officially ended on September 30, but was still active in parts of the country weeks later.

Brexit Deadline Extended to 2020

October 28

European Union leaders agreed to extend the deadline for the United Kingdom's exit from the EU to January 31, 2020. European Council President Donald Tusk described the new date as a "flextension," meaning the U.K. can leave earlier if a deal on the terms of withdrawal is approved by Parliament. Thus far, this has proved to be easier said than done. Despite months of assurances from Prime Minister Boris Johnson that the U.K. would leave the European Union on October 31, whether a deal was in place or not, opposition in Parliament continues to create an impasse. Brexit's fate now rests on the results of the next general election, which will be held on December 12.

Australia Faces Wildfire Threat

November 10

Wildfires raged throughout the Australian states of Queensland and New South Wales, prompting officials to declare states of emergency and call for evacuations as potentially "catastrophic" conditions worsened. To date, three people have been killed during this year's wildfire season as hundreds of fires burned more than 2.5 million acres of farmland and brush. Although fires occur regularly during the summer in Australia, many experts believe that the early arrival and intensity of this year's fires is due to the effects of climate change. ■

SHUTTERSTOCK/JOHN GOMEZ

The Leading Reference Source For Risk Management Professionals

CONTRIBUTE YOUR DATA TO THE

RIMS BENCHMARK SURVEY

AND RECEIVE A COPY AT NO COST!

The RIMS Benchmark Survey provides a unique window into the commercial insurance market. Seen against the backdrop of industry economic data, change in TCOR offer insights into the forces at work in the insurance industry. Armed with this information, insurance buyers are better positioned to design their risk financing programs, budget insurance costs, report more effectively to senior management, and negotiate with carriers.

THE 2019 SURVEY SHOWED:

- The P/C industry had a profitable 2018.
- TCOR was higher in 2018, largely due to rising insurance rates.
- For casualty lines, higher TCOR is in part a response to a higher frequency of very large losses.
- Property TCOR rose despite a significant decrease in catastrophe losses in 2018.
- Cyber insurance remains a major success story for insurers.

The Survey is based on 16,000+ insurance and represents more than $3.95 billion in premium. What trend will we see in 2020? Submit your data now, and get your copy of the 2020 RIMS Benchmark Survey free!

WHY CONTRIBUTE? SIMPLE–THE SURVEY ANSWERS THE QUESTIONS YOU CAN'T ASK ANYWHERE ELSE:

- How does the price I'm paying compare?
- Am I buying the right amount of insurance?
- What are others buying that I'm not?
- Who's writing the most of a specific type of coverage?

Get your questions answered. Submit your data and get your copy of the leading reference source for risk management professionals.

RIMS®
the risk management society

LEARN MORE AT WWW.RIMS.ORG/BENCHMARK

ENEMY OF THE STATE

Ransomware Surges Against State and Local Governments in 2019

by Hilary Tuttle and Adam Jacobson

THIS YEAR MARKS THE 30TH ANNIVERSARY of the first ransomware attack, a 1989 virus called the AIDS Trojan that targeted AIDS researchers. While the strategy went largely unused for some time, ransomware has surged over the past several years, becoming one of the most well-known threats in cyberrisk today. This year saw a notable increase in ransomware activity specifically among public entities, as a number of cities found themselves in the crosshairs of cybercriminals. The lessons learned from these attacks can help risk managers in understand the resulting risks and prepare for future threats.

SHUTTERSTOCK/WHITE MOCCA

Across the United States, cities are grappling with the risk of ransomware, a type of malware that encrypts an entity's data, allowing attackers to extort the victim for payment via cryptocurrency by threatening to release or destroy the data and incapacitating operations. By the beginning of November, cybersecurity company Barracuda reported that more than 70 U.S. cities had been the victims of ransomware attacks in 2019, the majority of which have less than 50,000 residents. StateScoop, a technology and government-focused media outlet, estimated the number to be even higher at 99. Municipalities are being targeted with growing frequency because of their fairly weak IT security practices, as well as the outsized attention and urgency that shutting down cities' systems can elicit. Additionally, cities often have limited budgets and technical staff, and may not have insurance to cover the attacks, leaving them exposed to exorbitant ransom or recovery costs.

In one of the first high-profile attacks on a major city, the government of Atlanta was hit with a ransomware attack in March 2018 that crippled the city's computer systems, forcing administrative offices to conduct business by pen and paper or even shutter altogether. The hacker or hackers asked the city to pay around $52,000 in bitcoin, but the city refused, leaving it scrambling to restore and protect its systems. Over a year later, that process has not yet fully ended. Atlanta officials have estimated that the recovery and cost of lost business could exceed $17 million.

Similarly, Baltimore suffered a ransomware attack in May 2019, with the hackers reportedly demanding 13 bitcoins (around $76,000 at the time) and shutting down many of the city's essential systems. Baltimore's government also refused to pay, opting to rebuild its computer systems instead. Its budget office has estimated that the city will have to pay at least $18.2 million over the course of recovery, factoring in both direct costs and lost revenue.

And in August, 22 small towns in Texas were reportedly targeted in a coordinated ransomware scheme, with the attacker demanding a collective ransom of $2.5 million, according to the mayor of Keane (one of the towns affected). A spokesperson for the Texas Department of Information Resources said that he was unaware of any of the towns paying the requested ransoms, and it has not been revealed if any data was permanently lost.

RESPONDING TO RANSOMWARE

Municipalities and other entities hit with ransomware face a dilemma. They can either pay the ransoms and hopefully recover data and restore operations quickly, or they can undertake the often-laborious process of recovering files from backups or investigating the type of ransomware and attempting to decrypt the hijacked files by themselves or with help from IT contractors. Since the recovery process can take longer—sometimes even weeks or months—many victims opt for paying the ransom, despite the risk of the attacker reneging on the promise to decrypt the captured data. Some insurance companies covering losses from ransomware incidents have reportedly advocated paying the ransom, cutting probable recovery time and allowing them to pay out a smaller sum than if they had to cover lost revenue from a longer business interruption.

However, the FBI recommends against victims paying attackers because it does not guarantee the return of their data and may encourage more crime. According to the FBI's Internet Crime Complaint Center, "Paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals." Cybersecurity firm Recorded Future reported that only around 17% of affected cities pay ransoms. In July, the U.S. Conference of Mayors, which represents mayors of cities with populations over 30,000, passed a resolution sponsored by Baltimore's mayor opposing payment to ransomware attackers, which stated that municipalities have "a vested interest in de-incentivizing these attacks to prevent further harm."

The best way to avoid becoming the victim of ransomware is to invest in IT security before

THE YEAR IN RANSOMWARE

Average costs

- Q3 2018: **$5,973**
- Q4 2018: **$6,733**
- Q1 2019: **$12,762**
- Q2 2019: **$36,295**

Attack vectors

- **59.1%** Remote desktop protocol (RDP) compromise
- **34.1%** Email phishing
- **6.8%** Software vulnerability

Average number of days a ransomware incident lasts: **9.6 days**

Age of vulnerabilities: **31.5% of the vulnerabilities exploited were over 4 years old**

Source: *Coveware; RiskSense*

an incident occurs, particularly by patching vulnerabilities and updating systems regularly. Cybersecurity company RiskSense examined 57 vulnerabilities that hackers exploited to infect systems with ransomware and found that 31.5% were unpatched vulnerabilities from 2015 or earlier, with some even dating back as far as 2010. Audits of Atlanta's computer systems before it was attacked showed thousands of potential vulnerabilities, including outdated software and a lax update policy that was habitually ignored.

Ensuring that the organization is thoroughly backing up its data also allows it to restore systems more quickly if compromised. These backups should be tested and updated often, while also making sure that they are not connected to the systems they are backing up by storing them elsewhere, including in the cloud or offline. Baltimore reportedly hosted its email almost entirely on an internal server before its systems were infected, and the city's IT department stored its data locally without backing any of it up. This made it easier for attackers to encrypt the city's system and may have led to permanent data loss.

A disaster recovery and business continuity plan is also an essential part of any organization's preparations for a ransomware attack. Knowing in advance who should handle specific parts of cyberattack response, such as isolating the affected systems or contacting law enforcement, can speed recovery efforts, whether the organization decides to pay the ransom or not. Establishing relationships and partnerships with the organization's insurer, internal and external cybersecurity personnel, and other essential stakeholders before an incident occurs will save the organization time and money in the event of an attack.

In addition to strengthening their IT systems, creating and enacting a recovery plan and choosing the right cyber insurance policy, organizations must ensure that they adequately train and test their staff to recognize phishing emails and messages that may contain malicious links or attachments. According to Coveware, 34.1% of ransomware cases in the second quarter of 2019 were the result of email phishing. No matter how strong security is, just one employee mistakenly clicking the wrong thing can allow attackers to cripple the whole enterprise.

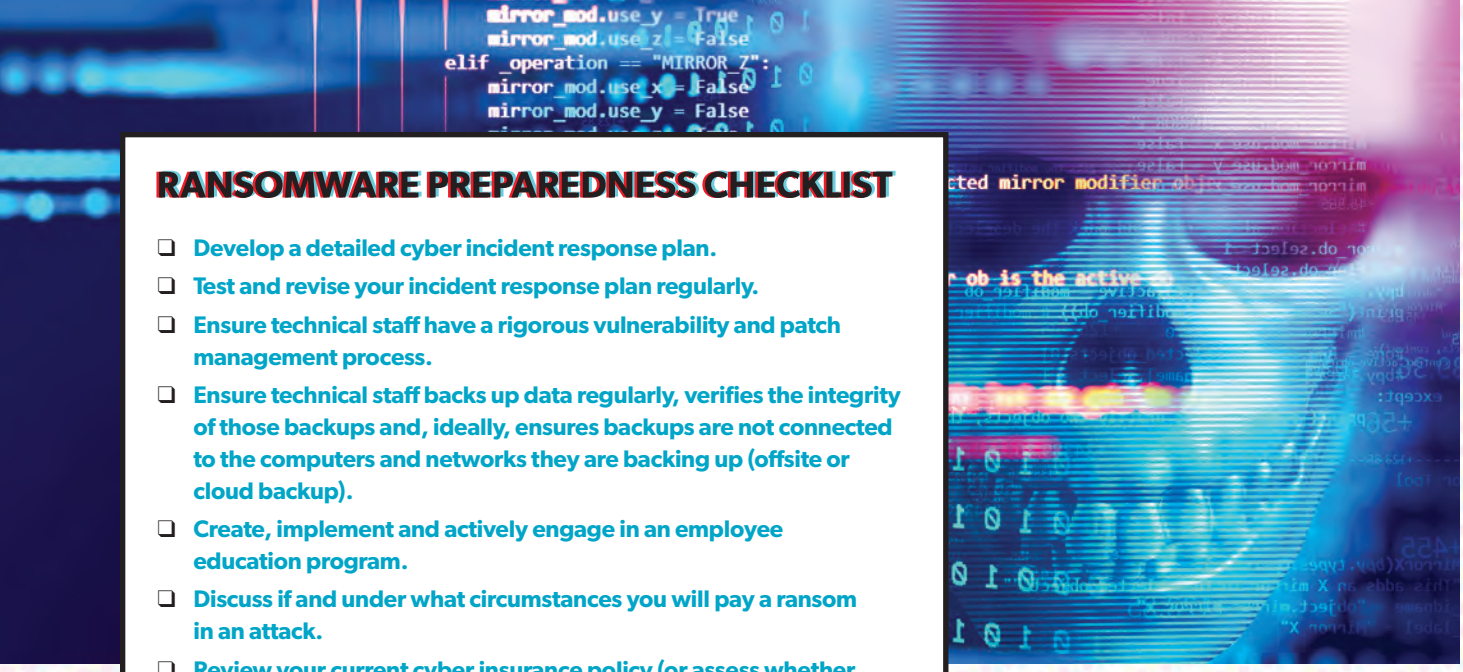
INSURANCE IMPLICATIONS

Coveware reported that, in the second quarter of 2019, the average ransom payment for all enterprises hit $36,295, a notable increase from the first-quarter average of $12,762. This was even more dramatic in the public sector, however, where victims paid an average ransom of $338,700—almost 10 times the global enterprise average.

More public entities are looking at cyber insurance options as the primary risk transfer option to defray these costs. The *Wall Street Journal* reported last year that a majority of the country's 25 most populous cities either had or were considering cyber insurance policies. As this year has demonstrated, such considerations are far from limited to the largest municipalities.

When Florida's Lake City and Riviera Beach fell victims to ransomware attacks this year, city leaders specifically noted their cyber insurance policies as a key factor in making the controversial decision to pay the ransoms. Both cities had policies that would pay the majority of the ransoms demanded—approximately $460,000 and $600,000, respectively—aside from a $10,000 deductible. Given the interruption of critical services and the costs of forensics and recovery efforts, officials felt that it was both faster and more cost-effective to pay the attackers for a decryption key.

"We pay a $10,000 deductible, and we get back to business, hopefully. Or we go, 'No, we're not going to do that,' then we



RANSOMWARE PREPAREDNESS CHECKLIST

- ❑ Develop a detailed cyber incident response plan.
- ❑ Test and revise your incident response plan regularly.
- ❑ Ensure technical staff have a rigorous vulnerability and patch management process.
- ❑ Ensure technical staff backs up data regularly, verifies the integrity of those backups and, ideally, ensures backups are not connected to the computers and networks they are backing up (offsite or cloud backup).
- ❑ Create, implement and actively engage in an employee education program.
- ❑ Discuss if and under what circumstances you will pay a ransom in an attack.
- ❑ Review your current cyber insurance policy (or assess whether to obtain one).
- ❑ Talk to your broker about the lines that could be triggered in a ransomware attack.
- ❑ Establish contacts with local law enforcement, such as the nearest FBI office.

spend money we don't have to just get back up and running," Lake City Mayor Stephen Witt later told ProPublica. "And so to me, it wasn't a pleasant decision, but it was the only decision."

After a ransomware attack hit LaPorte County, Illinois, in July, FBI negotiators brought in during the incident response process were reportedly able to negotiate a lower ransom than initially demanded. Officials then elected to pay a $130,000 ransom, of which county commissioners said $100,000 was set to be paid through an insurance policy with Travelers.

These decisions may have been informed, in part, by Baltimore still being mired in disruption from its attack, which struck just the month before. In October, the city purchased its own cyber insurance policy for the first time. In fact, it purchased two. After Baltimore's risk management office reviewed bids from 17 carriers, the city purchased policies with Chubb and AXA XL, each for $10 million in liability coverage after a $1 million deductible, for a total $835,000 in premiums. The policies are supposed to cover incident response, business interruption and ransom payments.

"As the world changes and as criminal acts change, you have to adjust," City Council President Brandon Scott told the *Wall Street Journal*. "This is an adjustment well worth it to protect the citizens of Baltimore and, most importantly, protect their taxpayer dollars in the event this happens again."

Not all may come down in favor of purchasing, however. The cases in Florida this year sparked considerable debate not only about the moral and practical questions of whether to pay a ransom, but of the insurance industry's role in the spate of ransomware attacks. Cases against public entities, by their very nature, require a different level of disclosure than is common in the private sector and draw considerable public attention—as do the ransoms insurers may cover. Many have argued that insurers' responses may be fueling the surge in attacks, and some experts in the cybersecurity industry and public sector have attempted to correlate the public payments to the rising ransom demands seen over the course of the year. Moving forward, public entity risk managers may need to be aware not only of the reputation risk associated with their crisis response and ransom payment decisions, but also potential questions about their risk mitigation and transfer decisions like purchasing cyber coverage.

The market itself will likely feel the effect of these payouts moving forward. As with most lines seeing an uptick in claims, it is reasonable to expect that public entities may see steeper rates for cyber insurance coverage or, at a minimum, increasing retentions. Both of the policies Baltimore recently purchased, for example, have a $1 million deductible. There remains enough capacity in the market and competition among cyber insurers, however, to help moderate potential rate increases.

Robert Parisi, managing director and cyber product leader at Marsh, told *Business Insurance* in July that the past 10 to 15 years have demonstrated the cyber insurance market's capacity to absorb some very large loss events, so he did not necessarily expect a sharp increase in rates in the near future. However, he added, "I think you will see carriers certainly ask more questions around whatever the latest issues were with regard to municipalities' ransomware. It's become a fairly common point of inquiry now across all industries, including municipalities."

Going forward, insurers will undoubtedly be taking a closer look at what technology infrastructure and cyberrisk management

SHUTTERSTOCK/WHITE MOCCA

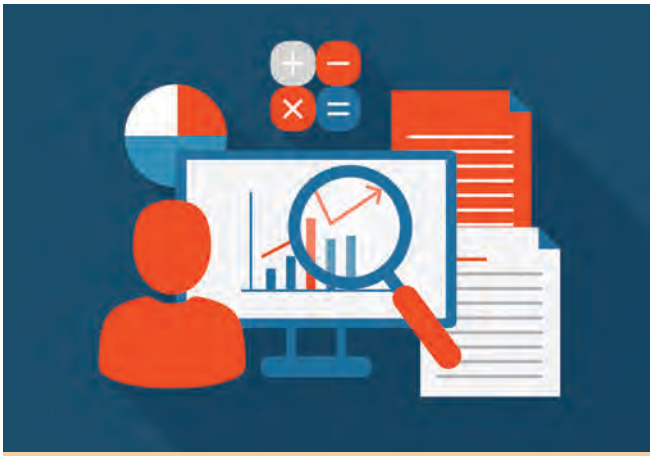
measures municipalities have in place. Heightened scrutiny from underwriters should underscore the importance of public entity risk managers focusing proactively on everything from detailed contingency planning to security awareness training for staff (see sidebar).

OTHER PUBLIC ENTITY THREATS ON THE HORIZON

Aside from municipalities, other public sector enterprises have endured more ransomware attacks this year or have been specifically put on notice about the threat, particularly education and healthcare entities. School systems and hospitals have been attacked throughout the year, crippling critical services and introducing acute concern about the security of key classes of protected data—personal information regarding children and personal health information. Advocacy groups in these sectors have turned greater attention to these issues, attempting outreach, education and preparation efforts among their stakeholders.

Worldwide, security and insurance experts have also increased their warnings about the potential peril to other key kinds of public entities like ports, where public entities' risk management poses particularly massive risk to both the public and private sectors. As the NotPetya attack demonstrated, the business interruption risks from attacks that hit the shipping industry and cripple ports can be particularly severe across the supply chain. A recent report produced by the University of Cambridge Centre for Risk Studies, Lloyd's and others found that a worst-case scenario attack on major Asia-Pacific ports could cause up to $110 billion in damages, for example, and given insurance penetration rates and the uncertainties inherent in non-affirmative or "silent" cyber coverage, 92% of the economic costs could be uninsured. Approximately 60% of losses would be due to business interruption or contingent business interruption, non-affirmative cyber represented up to 57% of losses, and economic losses could spread throughout the supply chain. Indeed, businesses along the supply chain faced 21% of claims in the scenario.

As the year closes, ransomware attacks show no sign of slowing. Rather, as these attacks continue to provide effective paydays for financially motivated criminals and the disruption or outright chaos other threat actors seek, public sector risk managers must refine their cyberattack prevention and response measures to prepare their organizations for tomorrow's threats. ■



EXCELLENCE IN RISK MANAGEMENT INDIA 2019

IN THE LATEST EDITION OF THE MARSH AND RIMS REPORT *Excellence in Risk Management India*, a vast majority of respondents emphasized wanting to forge stronger ties between risk management and strategic planning. Indeed, about two-thirds said that integrating risk management into strategic planning was their top investment priority for 2020. The next two top priorities may help: "upgrading risk management technology" and "improving data analytics." As risk professionals in India look to earn a seat at the table in enterprise-level conversations, making smart and timely investments in risk management technology may be a key differentiator in maturing risk management programs. "Risk managers who are able to show data-driven reasoning behind their recommendations are more likely to be effective partners across the business and sought out by other departments," the report noted. "At the same time, investing in more efficient technology can help automate some risk management tasks, potentially freeing time for risk managers to pursue more strategic issues." Currently, the biggest performance gap in organizations' risk management functions is implementing a formal enterprise risk management program, followed by "educating other (non-risk) employees on key risk management practices."

–Hilary Tuttle

CORPORATE INVESTIGATORS SEE MORE, COSTLIER CASES

E-discovery company H5 recently found that 60% of those involved with internal corporate investigations expect the number of investigations to increase over the next three years, citing increasing regulation, compliance pressures and companies' growth as the top driving factors. Nearly 30% of those surveyed said their company's investigation costs topped $1 million, and 17% said the costs were more than $6 million. Those located outside the United States reported that they spend more on investigations, with 21% saying that their company spends $10 million or more, compared to only 2% of U.S. respondents reporting the same spending level. The top three sources of these expenses were outside counsel (86%), analytics technology (59%) and e-discovery services (53%). Almost half of investigations relate to workplace issues like harassment, theft and discrimination, while regulatory/governmental issues make up an additional 24%. Cybersecurity investigations for issues like data breaches only accounted for 5% of investigations.

–Adam Jacobson

SECURITY SPENDING EXPECTED TO GROW

Worldwide spending on security products and services is expected to grow significantly over the next five years as companies look to address a wide range of security threats and regulatory requirements, according an International Data Corporation report. In 2019, companies will spend $106.6 billion on security-related hardware, software and services, an increase of 10.7% from 2018. By 2023, that number will reach $151.2 billion. The largest component of security spending this year—$47 billion—will be for services like managed security and threat monitoring, integration, consulting, and IT education and training. Nearly $38 billion will be allocated to software products, including for endpoint security, identity and digital trust, and security analytics, intelligence, response and orchestration. Hardware spending will amount to $21 billion, particularly for network security products like firewalls and intrusion detection and prevention technologies. Banking, manufacturing and federal government sectors are expected to be the top market segments.

–Morgan O'Rourke

ADOBE STOCK

LEARN RISK

RIMS EDUCATIONAL WORKSHOPS

Save $75 when you register 30 days in advance for any **RIMS workshop.**

Stay at the forefront of risk management trends and strategies at these upcoming in-person workshops. RIMS Members attend at special rates.

Enterprise Risk Management
January 23–24 | Los Angeles
February 20–21 | Orlando
March 2–3 | Montreal
March 12–13 | Cleveland
April 16–17 | Raleigh
May 1–2 | Denver

Fundamentals of Insurance*
January 27–28 | Washington, DC
February 24–25 | Cleveland
May 1–2 | Denver

Mastering Intelligence Risk Management Techniques
December 12–13 | New York City

Contractual Risk Transfer
January 23–24 | Toronto
March 19–20 | San Diego
May 1–2 | Denver
June 22–23 | New York City

Business Continuity Management
February 6–7 | San Diego
May 1–2 | Denver

Claims Management
March 23–24 | New York City
May 1–2 | Denver

Applying Enterprise Risk Management Theory
April 20–21 | New York City
May 1–2 | Denver

RIMS-CRMP Prep Workshop*
May 7–8 | Denver

Workers' Compensation Management*
June 25–26 | Washington, DC

***Also available as an online course.**

RIMS® *the* risk management society

Visit **www.RIMS.org/Workshops** to view our in-person and online education offerings.

Examining Future Risks

In a recent survey by AXA and Eurasia Group, over 1,700 risk experts from 58 countries identified the 10 major emerging risks that could have a significant impact on businesses in the next five to 10 years:

1. CLIMATE CHANGE
physical risks from extreme weather events; liability risks for carbon extractors and emitters; financial transition risks from moving to a lower-carbon economy

2. CYBERSECURITY RISKS
shutdown of essential services and critical infrastructure; cyber extortion and ransomware; identity theft; misinformation and loss of media independence; loss of privacy

3. GEOPOLITICAL INSTABILITY
rise of nationalism and populism; tensions between nation-states; decline of multilateralism; global shift of power to Asia

4. SOCIAL DISCONTENT AND LOCAL CONFLICTS
income gap and wealth disparities; migrations and territorial tensions; failure of institutions; water and food insecurity

5. NATURAL RESOURCES MANAGEMENT
loss of biodiversity, unsustainable land use, deforestation and desertification; over-consumption of natural resources; extraction of rare earth elements for low-carbon technologies

6. ARTIFICIAL INTELLIGENCE AND BIG DATA
liability challenges related to AI use; lack of interpretability of AI; existential threat of AI; AI investment gap between regions

7. POLLUTION
increased levels of air, water and soil pollution; plastic pollution and waste management; contamination of environment, water and food by nanoparticles; environmental damages from energy production

8. PANDEMICS AND INFECTIOUS DISEASES
new strains of infectious diseases; antimicrobial resistance and "super bugs"; changing patterns of infection due to climate change and global travel; declining vaccination rates

9. NEW THREATS TO SECURITY
cyber warfare and nation-state sponsored cyberattacks; evolving terrorist attacks by smaller groups and lone wolves; malicious use of new technologies; fake news

10. MACROECONOMIC RISKS
Chinese economy financial influences; Eurozone instability; emerging market crises; durable mass unemployment

Source: *AXA, Eurasia Group; Future Risks Report 2019*

TOP BUSINESS RISKS ON THE HORIZON

At the 2019 J.P. Morgan Asia Pacific CFO and Treasurers Forum in Shanghai in October, chief financial officers and group treasurers from 130 global corporations identified the key risk factors facing their business in the next six to 12 months:

Potential global recession..... **30%**
Impact of global tariffs..... **27%**
Emerging markets slowdown..... **24%**
Cyberthreats..... **10%**
Brexit/future of Eurozone..... **9%**

Source: *J.P. Morgan*

SHUTTERSTOCK; ADOBE STOCK

$109.8 BILLION

Worst-case economic cost of a hypothetical cyberattack on 15 major ports in Japan, Malaysia, Singapore, South Korea and China, according to a report from the Cyber Risk Management (CyRIM) project, a partnership between Nanyang Technological University, Lloyd's of London and others.

$8.3 BILLION

Insured losses from the attack, amounting to only 7.5% of the total cost. Business interruption and contingent business interruption claims would account for 60% of these losses.

Common Cybersecurity Challenges

Research from ISACA, CMMI Institute and Infosecurity Group found that risk professionals consider cybersecurity to be the most critical category of risk facing their organization both today and in the next 18 to 24 months. The most common cybersecurity challenges cited were:

Changes/advances in technology	**64%**
Changes in types of threats	**60%**
Too few security personnel	**52%**
Missing skills in existing cybersecurity team personnel	**51%**
Increased number of threats and/or increased frequency of threat occurrence	**45%**
Inadequate security budget	**39%**
Legal and/or regulatory challenges	**29%**
Lack of executive support/attention for security issues	**24%**
Lack of appropriate policy for key security areas	**24%**

EMERGING TECH RISKS

Respondents also identified which emerging technologies have increased the risks to their organizations as a result of their use:

Cloud	**70%**
Internet of things	**34%**
Machine learning and AI	**25%**
Blockchain (and/or cryptocurrency)	**13%**
5G	**6%**
Quantum computing	**5%**

Source: *ISACA, CMMI Institute, Infosecurity Group; State of Enterprise Risk Management 2020*

2019's Most Dangerous Celebrities

According to McAfee's annual report, U.S. internet searches for the following celebrities have the highest likelihood of exposing users to malicious content:


1. Alexis Bledel


2. James Corden


3. Sophie Turner


4. Anna Kendrick


5. Lupita Nyong'o


6. Jimmy Fallon


7. Jackie Chan


8. Lil Wayne


9. Nicki Minaj


10. Tessa Thompson

The riskiest celebrities vary by country. These were the most dangerous in their respective locations:

Australia:
John Oliver

France:
Jamel Debbouze

Germany:
Heidi Klum, Emilia Clarke (tie)

India:
MS Dhoni

Singapore:
Michelle Yeoh

Spain:
Camila Cabello

United Kingdom:
Caroline Flack

Source: *McAfee; 2019 Most Dangerous Celebrities*

SHUTTERSTOCK/MEGA PIXEL; DFREE; JSTONE; PHOTOCARIOCA; FEATURE FLASH; S_BUKLEY; JOE SEER; KYLE BESLER; TINSELTOWN

NEED A SOLUTIONS PROVIDER?
SEARCH RIMS MARKETPLACE,
THE INDUSTRY'S MOST COMPREHENSIVE BUYER'S GUIDE

BROWSE PRODUCTS

VIEW VIDEOS

READ CONTENT

Find a provider that'll help your company effectively minimize risk. Browse robust profiles with company descriptions, products, whitepapers, articles, videos, and more. Begin your search at www.RIMSmarketplace.com.

Find providers in categories including:

>> Claims Services

>> Finance

>> Human Resources

>> Insurance Providers/Services

>> IT Services

>> Legal Services

>> Risktech

>> Software

RIMS marketplace

www.RIMSmarketplace.com

10,000+ ATTENDEES

400+ EXHIBITORS

70+ COUNTRIES

300+ SPEAKERS

RIMS2020 DENVER

MAY 3-6

REGISTRATION IS OPEN

WHY SHOULD YOU ATTEND?

RIMS 2020 is the largest risk event of the year. You'll find an unprecedented number of sessions across a wide range of risk-related topics. In addition to in-depth sessions, there are shorter presentations in the Thought Leader Theater, Global Studio, Career Lab, Innovation Hub, and Wellness ZENter. Walk the Marketplace aisles to meet with your providers and discover new ones.

www.RIMS.org/RIMS2020