Cyber Security

An intelligence security firm recently reported on a new malware attack aimed at gathering personal information and blackmailing the user to divulge sensitive corporate information. The report states that cybercriminals are using popular adult and gaming websites to deliver this malware. Its goal is to gather family and workplace information about the user and use it to extort employer data or manipulate the victim into conducting operations that are harmful to the employer. The malware incorporates a plug-in that allows the criminal to operate the webcam without the user's knowledge to obtain sensitive or compromising videos that can strengthen the extortion scheme. According to Liam Tung, "The webcam malware could blackmail you into leaking company secrets," (zdnet.com [Jul. 18, 2016]).

Last year the FBI reported a 53 percent increase in economic espionage, costing U.S. businesses billions of dollars.

The insider threat is particularly attractive to cybercriminals because the victims typically have ready access to a wealth of information. IBM's 2015 cybersecurity report found that malicious insiders were responsible for more than 30 percent of data breaches.

A disturbing element of the malware is its ability to take over the user's webcam. Portable laptops can be a particular concern as they are often used in private places like hotel rooms or bedrooms. The images gathered, including images of employees changing their clothes or engaging in private activities, can be used for extortion purposes. A camera can also discover organizational data.

Some malware attacks may produce error messages when the webcam function is triggered, and many users will see an LED light when the camera is functioning. However, some hackers have been able to disable this light, so the attack goes completely unnoticed. A good anti-virus software and/or firewall can prevent outside intruders from breaking into your system, but they certainly are not infallible. The most effective way to protect yourself is by unplugging the camera from the USB port, or for embedded cameras, covering the lens with a piece of tape, a sticky note, or a penny.

A security software developer recently reported an encouraging finding in its analysis of malware in the U.S. After studying millions of infected personal computers, they found the rate of malware infection decreased 47.3 percent in the first half of 2016 when compared to the first half of 2015. This is the lowest rate of infection since April of 2013.

Researchers credit the rate drop to better antivirus software, more secure web browsers with regular security updates, and increased user awareness of common behaviors that result in infection. Also noted is the growing tendency to use mobile devices for internet tasks, leading to less time spent on a PC. Recent arrests of notorious Russian hackers could have some influence on the drop in malware, although inevitably there seems to be another criminal group ready to take the place of each one that is dismantled.

The experts are quick to temper the good news by reminding us that the overall number of malware infections remains at an all-time high. They also point out that users should stay vigilant of ransomware attacks. Reports show ransomware numbers are growing quickly, up 119 percent from 2015. *(Andy Patrizio "Malware infections drop in first half of 2016," www.networkworld.com [Jul 13, 2016].)*

Web browser developers are becoming more efficient in locating vulnerabilities and releasing updates to patch the holes in their browsers. For that reason, updating your browser and other software must be an on-going process. Once a vulnerability is detected and a patch is released, cybercriminals will move to exploit another weakness.

Effective data security is an ongoing endeavor and requires persistence. Employers must continually train their employees on safe usage behaviors, including regular software updates. In addition, make sure your system security policies include prevention measures as well as response procedures in the event a computer is infected.

Police Immunity from Civil Liability Resulting from Vehicular Chases Rosemary Morgan, et al. v. Beaumont Police Department, et al.

Court of Appeal, Fourth Appellate District (April 4, 2016)

Police departments have historically enjoyed statutory immunity under the vehicle code from any civil lawsuits resulting from injuries sustained during vehicular chases. This case concerns the burden the police department must carry to continue to enjoy the statutory immunity under the vehicle code for damage inflicted during vehicular pursuits.

Just before noon on March 17, 2011, Officer Brian Stehli was monitoring traffic on a city street when he saw a silver pick-up truck drive by with a large crack in its front windshield and a broken tail light. Stehli pulled behind the pickup. After calling-in the pickup's license plate number to dispatch, Stehli activated the lights and used the air horn once on his police cruiser as he followed behind the pickup. Instead of stopping, however, the driver of the pickup, later identified as Thomas Durnin, accelerated. This led to a high speed car chase in which both Durnin and Stehli reached speeds of up to 90 miles per hour. After a 12 minute car chase, Durnin's vehicle crossed a double yellow line and crashed head-on into another vehicle driven by Mike Morgan. Morgan subsequently died from the injuries he sustained in the crash, while Durnin was convicted of second degree murder, among other things.

The widow and daughter of Morgan filed a complaint, which contained an allegation of wrongful death against the City of Beaumont and the Beaumont Police Department (BPD) (collectively Defendants). Defendants filed a motion for summary judgment (MSJ) pursuant to Vehicle Code section 17004.7, which immunizes public entities from liability for injuries resulting from police pursuits of suspected criminals. Defendants stated that they had a "policy and procedure" in place according to the statute regarding vehicle pursuits of suspects. The trial court granted defendants' MSJ after finding defendants had a policy and procedure in place and therefore the immunity under section 17004.7 applied.

§17004. A public employee is not liable for civil damages on account of personal injury to or death of any person or damage to property resulting from the operation, in the line of duty, of an authorized emergency vehicle while responding to an emergency call or when in the immediate pursuit of an actual or suspected violator of the law, or when responding to but not upon returning from a fire alarm or other emergency call.

§17004.7. (a) The immunity provided by this section is in addition to any other immunity provided by law. The adoption of a vehicle pursuit policy by a public agency pursuant to this section is discretionary.

Continued on page 32

Managing Risk [continued]

(b) (1) A public agency employing peace officers that adopts and promulgates a written policy on, and provides regular and periodic training on an annual basis for, vehicular pursuits complying with subdivisions (c) and (d) is immune from liability for civil damages for personal injury to or death of any person or damage to property resulting from the collision of a vehicle being operated by an actual or suspected violator of the law who is being, has been, or believes he or she is being or has been, pursued in a motor vehicle by a peace officer employed by the public entity.

(2) Promulgation of the written policy under paragraph (1) shall include, but is not limited to, a requirement that all peace officers of the public agency certify in writing that they have received, read, and understand the policy. The failure of an individual officer to sign a certification shall not be used to impose liability on an individual officer or a public entity.

(c) A policy for the safe conduct of motor vehicle pursuits by peace officers shall meet all of the following minimum standards:

(1) Determine under what circumstances to initiate a pursuit. The policy shall define a "pursuit," articulate the reasons for which a pursuit is authorized, and identify the issues that should be considered in reaching the decision to pursue. It should also address the importance of protecting the public and balancing the known or reasonably suspected offense, and the apparent need for immediate capture against the risks to peace officers, innocent motorists, and others to protect the public.

(2) Determine the total number of law enforcement vehicles authorized to participate in a pursuit. Establish the authorized number of law enforcement units and supervisors who may be involved in a pursuit, describe the responsibility of each authorized unit and the role of each peace officer and supervisor, and specify if and when additional units are authorized.

(3) Determine the communication procedures to be followed during a pursuit. Specify pursuit coordination and control procedures and determine assignment of communications responsibility by unit and organizational entity.

(4) Determine the role of the supervisor in managing and controlling a pursuit. Supervisory responsibility shall include management and control of a pursuit, assessment of risk factors associated with a pursuit, and when to terminate a pursuit.

(5) Determine driving tactics and the circumstances under which the tactics may be appropriate.

(6) Determine authorized pursuit intervention tactics. Pursuit intervention tactics include, but are not limited to, blocking, ramming, boxing, and roadblock procedures. The policy shall specify under what circumstances and conditions each approved tactic is authorized to be used.

(7) Determine the factors to be considered by a peace officer and supervisor in determining speeds throughout a pursuit. Evaluation shall take into consideration public safety, peace officer safety, and safety of the occupants in a fleeing vehicle.

(8) Determine the role of air support, where available. Air support shall include coordinating the activities of resources on the ground, reporting on the progress of a pursuit, and providing peace officers and supervisors with information to evaluate whether or not to continue the pursuit.

(9) Determine when to terminate or discontinue a pursuit. Factors to be considered include, but are not limited to, all of the following:

(A) Ongoing evaluation of risk to the public or pursuing peace officer.
(B) The protection of the public, given the known or reasonably suspected offense and apparent need for immediate capture against the risks to the public and peace officers.
(C) Vehicular or pedestrian traffic safety and volume.
(D) Weather conditions.
(E) Traffic conditions.
(F) Speeds.
(G) Availability of air support.
(H) Procedures when an offender is identified and may be apprehended at a later time or when the location of the pursuit vehicle is no longer known.

(10) Determine procedures for apprehending an offender following a pursuit. Safety of the public and peace officers during the law enforcement effort to capture an offender shall be an important factor.

(11) Determine effective coordination, management, and control of interjurisdictional pursuits. The policy shall include, but shall not be limited to, all of the following:

(A) Supervisory control and management of a pursuit that enters another jurisdiction.
(B) Communications and notifications among the agencies involved.
(C) Involvement in another jurisdiction's pursuit.
(D) Roles and responsibilities of units and coordination, management, and control at the termination of an interjurisdictional pursuit.

(12) Reporting and postpursuit analysis as required by Section 14602.1. Establish the level and procedures of postpursuit analysis, review, and feedback. Establish procedures for written postpursuit review and followup.

(d) "Regular and periodic training" under this section means annual training that shall include, at a minimum, coverage of each of the subjects and elements set forth in subdivision (c) and that shall comply, at a minimum, with the training guidelines established pursuant to Section 13519.8 of the Penal Code.
(e) The requirements of subdivision (c) represent minimum policy standards and do not limit an agency from adopting additional policy requirements. The requirements in subdivision (c) are consistent with the 1995 California Law Enforcement Vehicle Pursuit Guidelines developed by the Commission on Peace Officer Standards and Training pursuant to Section 13519.8 of the Penal Code that will assist agencies in the development of their pursuit policies. Nothing in this section precludes the adoption of a policy that limits or restricts pursuits.
(f) A determination of whether a public agency has complied with subdivisions (c) and (d) is a question of law for the court.
(g) This section shall become operative on July 1, 2007.

The Court of Appeal reversed, finding that defendants had failed to provide sufficient evidence to establish as a matter of law that BPD had "promulgated" its vehicle pursuit policy as required under section 17004.7. First, the Court looked at the statute in question and noted that the statute required that all peace officers certify in writing that they have "received, read, and understood" the policy.

The Court then looked at the holding in Nguyen v. City of Westminster (2002) 103 Cal.App.4th 1161 (Nguyen). In Nguyen, an individual was killed after police officers chased a stolen van into a high school parking lot as classes were ending. The van struck a trash dumpster that hit the decedent. The Nguyen court "reluctantly" concluded summary judgment was properly granted under the former section 17004.7, which only required a department adopt a policy regarding vehicle chases. Following Nguyen, the Legislature amended § 17004.7 and the Court examined the legislative history of the amendment.

The Court then turned to the evidence that BPD had submitted in support of their MSJ, which outlined their procedure for promulgating their vehicle chase policy. BPD declared that they had hired a third party, Lexipool Risk Management Service (Lexipool), to assist with policy drafting and adopting. Once a new policy was created, or a revision to a policy was made, BPD would e-mail its officers, notifying them of the change and directing them to access the policy directly through Lexipool, or by accessing the department's shared drive. Employees would then acknowledge receipt of the policy by email, although those emails were not maintained or preserved. BPD also declared through one of its officers that the "vast majority" of officers complied with the email

Continued on page 38

acknowledgement described above. The Court found that evidence of "receipt" of an email was insufficient to meet the requirements of the amended statute that all officers certify they had "received, read and understood" the policies in question.

The Court of Appeal thus held that an agency's vehicle pursuit policy is not promulgated within the meaning of § 17004.7(b) (2) unless, at a minimum, "all" of its peace officers "certify in writing that they have received, read, and understood the policy."

The Court declined to address the other ground for the appeal that the BPD training program did not meet the requirements of § 17004.7, which also requires periodic training on the vehicle pursuit policy. Finally, the Court rejected the BPD's argument that summary judgment was properly granted because the trial court alternatively found that the accident did not occur as a result of any negligence on the part of the officer as he had terminated the chase before the collision. The Court ruled that there was a triable issue of fact on this point, as the high speed chase had gone on for 12 minutes, and because Durnin still believed he was being pursued by police at the time of the collision.

COMMENT

For public entities, this case serves as a warning to have a robust policy regarding vehicle pursuits and to ensure that all officers receive it, read it, understand it, and undergo periodic training on the pursuit policy. This will ensure the department enjoys the shield of immunity while simultaneously – according to the legislature – reducing the number of innocent bystanders needlessly injured in the course of vehicular pursuits.

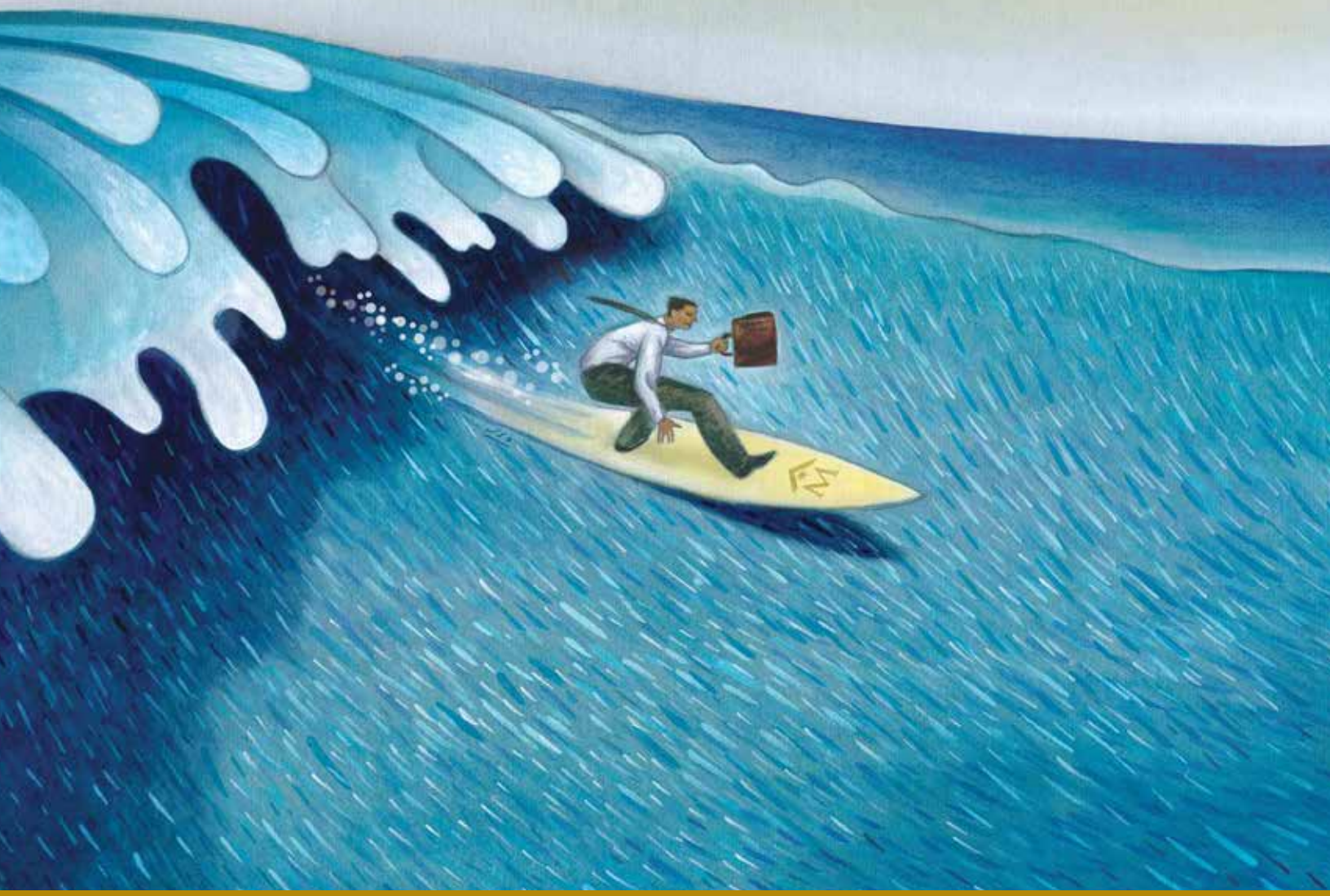
For more information or to submit questions, please contact SDRMA Chief Risk Officer Dennis Timoney at 800.537.7790 or email Dennis at dtimoney@sdrma.org.

District **Snapshots**

Big Bear CSD celebrated 50 years of service! Congratulations on such a great milestone!

SDRMA

SPECIAL DISTRICT RISK MANAGEMENT AUTHORITY



Ready for every wave.

SDRMA offers a seamless extension of balance and agility. For 30 years, we've been helping California public agencies ride the changing waves of risk. Whatever the emerging trend or ongoing exposure, our unique combination of world-class consulting and technical experts stands superior on our members' behalf.

We serve as a single resource for all your coverage protection and risk-management needs. Visit our website at **www.sdrma.org** or call us at **800.537.7790** to learn more about our Workers' Compensation, Property/Liability and Health Benefits Programs.

SDRMA 2016 30 YEARS

A proud California Special Districts Alliance partner

Trusted Risk Management ∗ **800.537.7790** ∗ **www.sdrma.org**