SECURITY
MANAGEMENT

The Trouble with Technology

This collection of articles from the security profession's premier publication examines the pitfalls or downright security dangers presented by technological advancement.

SECURITY MANAGEMENT

Future Proof

Most agree that passwords alone are not an ideal authentication method. But what should replace them?

By Megan Gates

During Operation Overlord, Allied forces needed a way to identify and authenticate friendly troops when they could not see them. The solution was to issue signs and countersigns—code words that could be used in a sentence during the Battle of Normandy in 1944 to communicate soldiers were on the same side and not to open fire.

One such sign–countersign code was Flash–Thunder. A soldier would call out a sentence using the code word "flash." The other soldier would respond with a sentence using the word "thunder," and the first soldier would say back a phrase using the word "welcome"—indicating that his use of the word flash was legitimate.

Today, methods of authentication are more sophisticated but tend to rely on three factors—something we know, something we have, or something we are—to gain access. But these authentication methods depend heavily on what some see as an outdated and insecure tool: passwords.

"Passwords are not providing sufficient protection," wrote Andrew Shikiar, executive director and chief marketing officer of the Fast Identity Online (FIDO) Alliance, and Adrien Ogee, project lead for the World Economic Forum's Platform for Shaping the Future of Cybersecurity and Digital Trust, in a recent paper Authentication: The Next Breakthrough in Secure Digital Transformation.

FIDO was created in 2012 to address interoperability among authentication technologies. It has since released standards to create stronger authentication mechanisms that reduce reliance on passwords.

"Authentication is so much broader than passwords," Shikiar and Ogee explained. "It is the foundation of digital trust, an enabler of cybersecurity in the digital economy and of the Fourth Industrial Revolution: in short, authentication is a critical enabler of the future."

THE PROBLEM

Accessing online and internal systems using usernames and passwords is an authentication method that's been mainstream since the 1980s. However, it puts the onus on users to create strong, unique passwords for hundreds of accounts.

"Passwords force users to create and memorize complex amalgams of letters, numbers, symbols, and cases; to change them frequently; and to try not to re-use them across accounts," Shikiar and Ogee wrote. "Numerous studies and cumulated company experience prove that individuals don't think or act this way. As a result, they re-use the same

passwords repeatedly, which is one reason why passwords are at the core of the data breach problem."

In 2017, the average employee used 191 passwords to access accounts, according to the Password Exposé published by LastPass—a password manager. Considerable time is also spent entering or resetting passwords each year; FIDO found that employees averaged 11 hours per year spent on these activities.

"Authentication is so much broader than passwords,"

"For a company of 15,000 employees, on average, this represents a direct productivity loss of $5.2 million," Ogee and Shikiar explained.

IBM also found that just 42 percent of millennials and 49 percent of people 55 and older reported using complex passwords.

This raises concerns because passwords are one of the most commonly compromised information sets in a data breach that can then be used by malicious actors.

"The vast majority of data breaches stem from weak or stolen authentication credentials," Shikiar and Ogee wrote. "Today, credential stuffing attacks, i.e. attacks leveraging stolen credentials, are so common that over 90 percent of all login attempts on major retail sites are malicious, with average success rates around 1 percent."

And this level of fraud has a major economic impact on organizations and compromised users. "In the past six years, USD 112 billion has been stolen through identity fraud, equating to USD 35,600 lost every minute," according to IBM Security's Future of Identity study.

"Recent data breaches have been a resounding wake-up

call to the fact that new methods are needed to validate our identities online," IBM said. "In an era where personal information is no longer private, and passwords are commonly reused, stolen, or cracked with various tools, the traditional scheme of accessing data and services by username and password has repeatedly shown to be inadequate."

Users are also increasingly preferring more secure methods of authentication to access accounts related to their financial activity. In a survey of roughly 4,000 people around the globe, IBM found that 70 percent ranked security over convenience for accessing banking websites and applications—as opposed to social media accounts where

Users are also increasingly preferring more secure methods of authentication to access accounts related to their financial activity.

only 34 percent ranked security ahead of convenience.

"It turns out that users place more value on certain types of data, and as a result will prioritize security and privacy in some cases, while prioritizing speed and convenience in others," according to IBM.

However, this may be misguided because many users are using their Facebook and Twitter accounts to authenticate and access other applications and services.

"Many popular services that house sensitive information, like delivery services, online shopping, and dating apps, encourage users to log in using their social accounts," IBM wrote. "Therefore, if one of these social accounts is compromised, there could be a domino effect on how many additional accounts may also fall into the attacker's hands."

This plays into a broader lack of trust and confidence in organizations' ability to keep information, like passwords, secure.

"Individuals are wary about giving out too much personal information; partners fear the loss of confidential information and business processes; and global enterprises risk the loss of reputation and revenues when systems and customers are compromised," Ogee and Shikiar wrote.

THE SOLUTION

These factors are coming together to push innovators to develop and implement new authentication methods that users are receptive to, including biometrics, security keys, QR code authentication, behavioral analysis, and zero-knowledge proofs.

In just a few years, consumers have already become accustomed to using biometrics—such as facial recognition and fingerprints—to access their smartphones. Apple announced its version of the solution, Face ID, in 2017 when it unveiled the iPhone X.

Along with touting the ease of using the facial recognition scanning technology to unlock iPhones, Apple also stressed how the biometric data is securely stored and processed to prevent compromises.

"All saved facial information is protected by the secure enclave to keep data extremely secure, while all of the processing is done on-device and not in the cloud to protect user privacy," Apple said in a press release. "Face ID only unlocks iPhone X when customers look at it and is designed to prevent spoofing by photos or masks."

The technology follows the six building blocks that FIDO identified as necessary for building an authentication program capable of passing the test of time: security, privacy, sustainability, inclusiveness, scalability, and user experience.

"Security technologies tend to be short-lived and evolve rapidly," Shikiar and Ogee explained. "Whether opera-

tional one year or 10 or more, cyber criminals are generally adept at finding ways to circumvent security controls. Authentication technologies are no exception. It is consequently critical to build out a long-term security strategy."

FIDO, which was originally founded by PayPal, Lenovo, Nok Nok Labs, Validity Sensors, Infineon, and Agnitio, released the FIDO Universal Authentication Framework (UAF) and the FIDO Universal 2nd-Factor (U2F) in December 2014 to help guide developers and transition away from password usage.

Since then, numerous other companies have come on board and released password-alternative authentication methods that meet FIDO standards.

For instance, in 2019 Microsoft made FIDO authentication a fundamental component of its efforts to provide a seamless, password-free login experience. The U.S. General Services Administration also enabled FIDO authentication for login.gov, the single sign-on website for U.S. public and federal employees to interface and transact with federal agencies online.

Additionally, Google added FIDO support across its platforms—including the ability to use Android phones and iPhones as a physical security key for its Advanced Protection platform. The platform has traditionally required a security key as an authentication method.

"According to a study we released last year, people who exclusively used security keys to sign into their accounts never fell victim to targeted phishing attacks," wrote Shuvo Chatterjee, product manager for Google's Advanced Protection Program, in a blog post. "But, using security keys can be a hurdle for users: they can be costly, and acquiring and keeping track of two extra pieces of hardware is a burden."

This led Google to create a method that allows a smart-

phone to act as a user's security key, in a way that is compliant with FIDO's standards.

"Everything becomes much simpler when the things we're already carrying around—our smartphones—have a built-in security key," Chatterjee explained.

Intuit also released a FIDO-approved passwordless authentication method across its mobile apps, which reduced sign-in times by 78 percent and successfully authenticated users 99 percent of the time. This marked an increase over the 80 to 85 percent authentication rate for SMS-based multifactor authentication Intuit was using previously.

"Never before have service providers and developers had the ability to enable convenient, cryptographically secure authentication to a user base this broad," Shikiar said in a statement. "Service providers are now taking advantage of these new capabilities on a global scale."

However, the transition away from using passwords is not where the development of new authentication methods will end.

"Criminals adapt and security controls tend to be short lived," Shakiar and Ogee wrote. "The future of authentication will take many paths, some that we are only starting to explore like blockchain-based self-sovereign identities and zero trust networks. But the immediate journey for platform businesses to embark on leaves passwords behind."

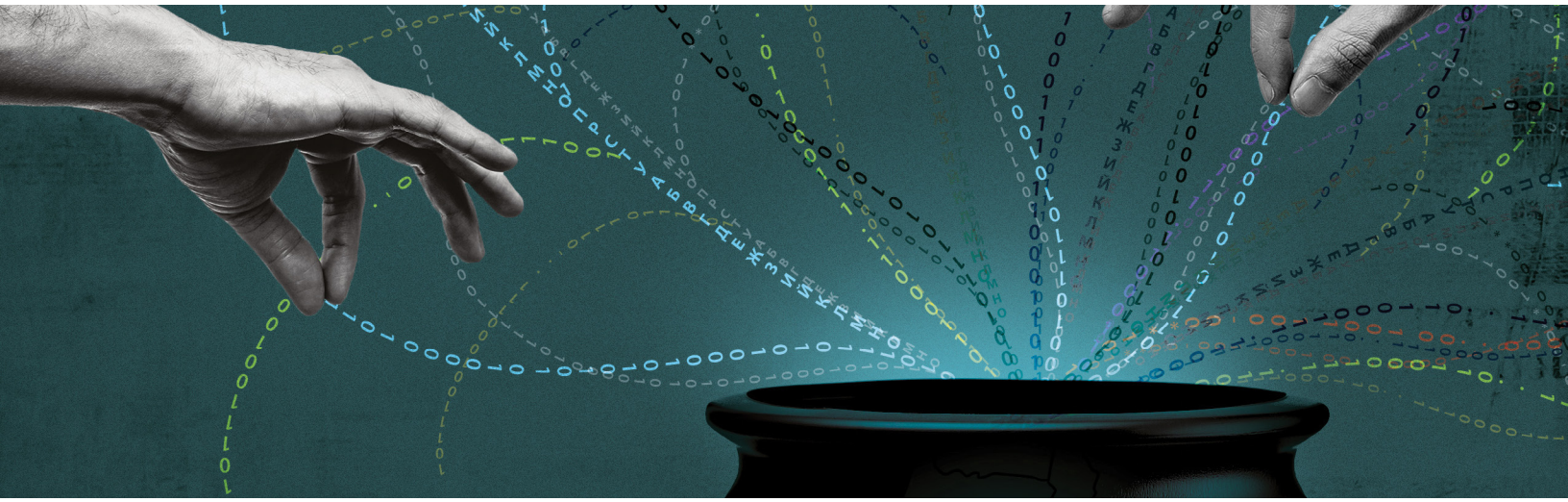
MEGAN GATES IS EDITOR-IN-CHIEF OF SECURITY TECHNOLOGY. CONNECT WITH HER AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.

SECURITY MANAGEMENT

Privacy in Practice

This summer, enforcement began for the first U.S. state-level comprehensive privacy law, creating opportunities and challenges for organizations subject to compliance.

By Megan Gates



Ashley LeMay and Dylan Blakeley had had enough. The wife and husband had purchased two indoor Amazon Ring security cameras for their home to make them feel safer and to help keep an eye on the couple's four daughters during LeMay's overnight shifts at a hospital.

This was especially important to the family because their middle daughter suffers from seizures, so the ability to be quickly notified if a medical emergency occurred at home was of paramount concern.

Unfortunately, while the cameras allowed LeMay and Blakeley to monitor their home, it also provided the same ability to a group of criminals who on 4 December 2019

breached the cameras and began live-streaming their feeds. They also played the song "Tiptoe Through the Tulips" into the home by using the cameras' two-way talk feature.

One of the couple's daughters heard the music and went to investigate the noise. After entering a room with a camera, the music stopped and a man's voice said, "Hello there." The voice then began to yell racial slurs at the girl, who left the room to tell Blakeley what happened. He later disabled the camera.

Data is today's gold. And as with gold, there's been a rush to mine, use, and sell our personal information.

Once LeMay and Blakeley found out that similar instances had occurred with other Ring cameras, they decided not to wait any longer for Ring to address the problem. Instead, they joined another couple in a class action lawsuit alleging that Amazon had shared their personal information to an unauthorized third party and failed to properly secure its products.

"Ring does not require users to implement two-factor authentication. It does not double-check whether someone logging in from an unknown IP address is the legitimate user," according to the filing. "It does not offer users a way to view how many users are logged in. It offers no protection from brute-force entries—mechanisms by which hackers can try an endless loop of combinations of letters and numbers until they land on the correct password to unlock an account. Even though these basic precautions are common and unexceptional security measures across a wealth of online services, Ring does not utilize them for its services."

The lawsuit was one of the first filed that alleged any kind of a violation of the California Consumer Privacy Act (CCPA). The law went into effect on 1 January 2020, but due to COVID-19 the California attorney general did not begin enforcement until 1 July 2020 and final regulations were approved 14 August 2020.

Under the CCPA, individuals have only a private right of action (grounds to file a lawsuit) if their personal data has been breached. Other cases must be brought by the Office of the California Attorney General. But cases like the one filed by LeMay and Blakeley show that individuals will seek claims under the CCPA—even before enforcement officially began.

"Additionally, we are seeing cases where consumers are attempting to extend the private right of action to other violations of the CCPA (e.g. failure to provide notice, as in the Ring case)," according to an analysis by Alex Scheinman, director at ACA Compliance Group, who oversees the company's General Data Protection Regulation (GDPR) data processing reviews and data privacy. "While the outcome of these cases is yet to be determined, including whether the consumers have standing to bring a suit, it is clear that consumers are availing themselves of this recourse mechanism and will likely continue to do so."

CCPA BASICS

The CCPA was passed by the California state legislature and signed into law by then Governor Jerry Brown in 2018. The law secured new privacy rights for California consumers and was the first of its kind in the United States.

Under the law, Californians have the right to know about the personal information a business collects concerning them and how it is used and shared; have the right to

delete personal information collected from them—with exceptions; have the right to opt-out of the sale of their personal information; and have the right to nondiscrimination for exercising their CCPA rights.

"For the first time in a legal regime, Americans, at least in California, have the right to tell a business that sells their information, don't," said California Attorney General Xavier Becerra in testimony before the U.S. Senate Committee on Commerce, Science, and Transportation.

Along with these rights for consumers, the CCPA also requires businesses to provide Californians with notices explaining their privacy practices, which has become critically important during the fight against COVID-19.

"...as we battle a pandemic that has moved so much of life online, companies know more about us, our children, our habits than ever before," Becerra explained. "That data is today's gold. And as with gold, there's been a rush to mine, use, and sell our personal information. Americans need robust tools that allow them to understand who has their data, what was collected, if it can be deleted, and how they can opt out of downstream selling."

The CCPA is not, however, as broad as a law that it is commonly compared to—the European Union's GDPR.

"Some folks call or refer to CCPA as an omnibus data protection law, akin to GDPR," says Caitlin Fennessy, research director at the International Association of Privacy Professionals (IAPP). "CCPA is focused to a much greater extent on the sale of personal data...it does not provide the full suite of fair information practices that privacy professionals are familiar with."

For instance, Fennessy says GDPR is premised on the requirement that organizations need to have a legal ba-

sis to process someone's data. But CCPA does not address whether it's legal for a business to process an individual's data; instead, it focuses on providing consumers with the ability to control whether their information is sold.

The penalties for violating the CCPA are still steep—civil penalties up to $2,500 for each violation or $7,500 for each intentional violation of the law. Given the population of California, approximately 39.5 million people as of 2019, these costs could add up quickly for organizations that commit violations.

And while the law is still very new, privacy professionals are watching closely to see whether other U.S. states propose and pass similar legislation and what developments occur in the courts.

Companies have one more driver to move to a state-of-the-art technology to protect user accounts.

"We are seeing a lot of linkage between allegations of violation of CCPA primarily on data breach or no opt-out of sale and lack of notice of collection," Fennessy says. "But very often plaintiffs are combining that with counts related to the unfair competition law in California and trying to link those two things to provide for a private right of action. We're waiting to see if that legal theory works or sticks."

This is the approach that LeMay and Blakeley's legal team is using in their class action lawsuit, which is currently winding its way through the California court system.

"As described herein, [Ring] advertised their products and services as enhancing security and safety, but in fact provided products and services that were highly vulnerable to hacking and that worsened the safety and securi-

ty of Plaintiffs and the Class Members," according to the suit, allegedly a violation of California's unfair competition law because Amazon falsely advertised its products.

AG FOCUS

Prior to the enforcement deadline, the California Office of the Attorney General undertook major conversations with stakeholders to craft the final regulations for CCPA. This included seven public forums, more than 300 letters, four public hearings, and an open comment period where more than 1,000 public comments were submitted.

After reviewing this information, the attorney general withdrew four provisions from CCPA regulations before finalizing them on 14 August 2020.

"In California, privacy is an inalienable right. Californians should control who possesses their personal data

"In California, privacy is an inalienable right. Californians should control who possesses their personal data and how it's used."

and how it's used," Becerra said in a statement. "With these rules finalized, California breaks ground and leads the nation to protect and advance data privacy. These rules guide consumers and businesses alike on how to implement the California Consumer Privacy Act. As we face a pandemic of historic proportions, it is particularly critical to be mindful of personal data security."

The first withdrawn provision was on a section of the law (Section 999.305) that prevented businesses from using consumers' personal information for a materially different purpose than what was disclosed when the business collected the information, unless it obtained consent from the consumers.

Another withdrawn provision would have required businesses' methods for opting out of data collection to be easy for consumers to follow and require minimal steps, along with a provision that would have required businesses that interact with consumers offline to provide offline notices about their ability to opt-out of data collection. Additionally, the attorney general withdrew requirements that allowed businesses to deny requests from authorized agents that do not submit proof that they are authorized to act on a consumer's behalf.

The Office of the Attorney General did not provide an explanation for why these changes were made, which has led privacy experts like Fennessy to ponder the decision.

"It could be as simple as they didn't hew to the exact letter of the law and the AG wanted to make sure they were able to defend that—that they had the authority to defend everything in the regulations," she adds.

Under the CCPA, the California attorney general is required to provide notice to organizations that are in violation of the law and give them 30 days to remedy those errors and become compliant. His office sent letters out after 1 July, as soon as it was legally able to do so, said Stacey Schesser, supervising deputy attorney general, California Department of Justice, in a panel discussion hosted by IAPP.

"There was a surprise that we were enforcing the law, but I think the attorney general has been quite forthcoming that July 1 starts enforcement," Schesser said, adding that if organizations fail to take steps to become compliant, the attorney general could open an investigation or file a lawsuit against them.

Organizations that receive these notices should take actions to become compliant and also notify the attorney general of the steps they have taken to become so, said

Travis LeBlanc, partner at Cooley LLP and member of the Privacy and Civil Liberties Oversight Board, in the panel. Taking these actions is critical, he added, because if the attorney general opens an investigation, it will not be limited to the original issues.

"They can start looking at broader consumer protection issues…and violations of other privacy statutes within California," LeBlanc said.

So far, Schesser said, the attorney general's office has focused its enforcement actions on businesses that operate online and needed to make actions and options available online for Californians to exercise their rights under CCPA.

"A central aspect of CCPA and one of the most robust rights CCPA affords Californians is the right to opt-out of the sale of personal information and the requirement that if a business is selling personal information that they have that 'Do Not Sell' link that's clearly and conspicuously posted on the homepage," Schesser said. "Given that that is really a unique aspect of this law—and one that is clearly spelled out in this statute—it would be appropriate to assume that businesses that are selling information and don't have that link should make sure to cure that as quickly as possible."

While the attorney general's office is spearheading its enforcement efforts, CCPA also allows Californians to file suit against a business if their nonencrypted and nonredacted personal information is leaked, such as in a data breach.

Under this private right of action, Californians can sue to recover damages between $100 and $750 per incident or actual damages—whichever is greater—along with injunctive or declaratory relief and any other relief the courts deem proper.

When assessing statutory damages, the court will consider a number of circumstances, including the number of violations; the willfulness of the defendant's misconduct;

the nature, seriousness, persistence, and length of time of misconduct; and the defendant's assets, liabilities, and net worth, according to the CCPA.

And while private right of action suits are meant to focus on this one area of liability, privacy and legal experts have seen a slew of lawsuits filed that expand upon this—including the Ring case.

In the IAPP panel discussion, Dominique Shelton Leipzig, partner, privacy and security, co-chair of ad tech privacy and data management at Perkins Cole, said that—as of July 2020—she is aware of 55 cases that have been filed utilizing a private right of action. Just one-third of those cases, however, allege violations of the CCPA explicitly. The rest mention the CCPA alongside unfair competition and other claims of California law violations.

FUTURE IMPACT

While many of the provisions in CCPA are focused on data collection and rights of Californians to be aware of those practices, there are also requirements for security.

The final regulations require businesses that collect Californians' data to implement "reasonable security measures to detect fraudulent identity- verification activity and prevent the unauthorized access to or deletion of a consumer's personal information."

Additionally, if a consumer has a password-protected account with a business, the business can use its existing authentication practices to verify that consumer's identity.

"If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person

about whom the business has collected information," according to the regulations.

This focus on verification and account protection is pushing organizations to explore using more advanced authentication methods, says Rolf Lindemann, vice president of products at Nok Nok Labs, Inc., and co-chair of the UAF Technology Working Group for the FIDO Alliance.

The FIDO Alliance is an open industry association focused on authentication standards to reduce reliance on passwords. It develops technical specifications for open, scalable, interoperable authentication methods to reduce reliance on passwords; operates industry certification programs to ensure adoption of those specifications; and submits technical specifications to recognized standards development organizations for formal standardization.

"Usernames and passwords, we can't argue that those are best practices for security," Lindemann says. "The nuance here is that companies have one more driver to move to a state-of-the-art technology to protect user accounts."

This is already happening in the financial sector where banks are requiring customers to use multifactor authentication methods to log in to their accounts. There's also growing interest in using biometrics for authentication, Lindemann adds, because FIDO helped create an ecosystem where a user's data is only uploaded to the device he or she is using to authenticate themselves—it is not transferred beyond that device, adding in an extra layer of security.

"When we designed FIDO in the first place, data privacy was a major concern and an important factor for us," Lindemann says. "We made sure that if you use FIDO, there is no need to store biometric data on the server side. There is no need to track the user beyond the data you collect from the user already. It's not adding another super cookie."

As consumers increasingly prioritize their privacy and

as new laws and regulations are adopted, Lindemann says organizations will be under greater pressure to adopt more secure methods for authentication to ensure compliance and trust.

Following California, Nevada and Maine have adopted comprehensive privacy laws; Connecticut, Louisiana, Massachusetts, North Dakota, and Texas set up task forces to craft comprehensive bills on privacy protections; and 16 other U.S. states had privacy legislation in process.

At the federal level, there is also increasing interest in Congress to pass greater privacy protections for Americans, such as the SAFE DATA Act (S. 4626) introduced by Roger Wicker (R-MS), chair of the U.S. Senate Commerce, Science, and Transportation Committee.

The bill would enshrine some of the same rights that the CCPA does for Californians, including the right to access, correct, delete, and transfer data collected by an organization. It would also require companies to minimize data collection, processing, and retention; hire data security officers and designate privacy officers; and conduct regular privacy impact assessments.

"The biggest new development that has impacted data privacy—as it has impacted so many facets of our life—is the COVID-19 pandemic, which has resulted in millions of Americans working from home," Wicker said during a Senate hearing about the need for federal level data privacy legislation. "The increased use of video conferencing, food delivery apps, and other online services increases the potential for privacy violations. The need to collect a great deal of data for contact tracing and to track the spread of the disease likewise raises privacy concerns if done improperly. For all of these reasons and more, the need for a uniform, national privacy law is greater than ever."

Privacy legislation at the U.S. federal level has routinely

stalled, however, because of issues identified in a Brookings Institution report published in June 2020. The report looked at Wicker's previous draft of the U.S. Consumer Data Privacy Act (USCDPA), which the SAFE DATA Act contains provisions of, and legislation introduced by U.S. Senator Maria Cantwell (D-WA), the Consumer Online Privacy Rights Act (COPRA).

"Although COPRA and USCDPA are promisingly similar in many aspects, stakeholders have staked out polar all-or-nothing positions on the two provisions where Wicker and Cantwell are the furthest apart—preemption and the private right of action," according to Brookings. "As long as these protagonists remain in their own corners, the broader privacy debate will be frozen and federal legislation stalled."

MEGAN GATES IS SENIOR EDITOR AT SECURITY MANAGEMENT. CONNECT WITH HER AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.

SECURITY MANAGEMENT

Monitoring Remote Workers

Monitoring tools can track productivity and guard against security threats, but employers should weigh the benefits against the legal risks.

By Dave Zielinski

Security Management has partnered with SHRM to bring you relevant articles on key workplace topics and strategies.

More employees are working from home, and more employers are keeping an eye on them through use of remote monitoring technologies. These tools perform multiple tasks, such as tracking keystrokes and measuring employees' active and idle time in key applications and websites. Monitoring tools also help companies enforce data security policies, and even take photos to see whether workers are sitting at their laptops at home.

But tracking tools aren't without risks. Workplace monitoring is subject to a variety of federal and state laws regarding when employees have a right to privacy and if

and when they must be notified that they're being monitored. From a legal perspective, disclosing surveillance is the smartest tactic. Letting employees know that they will be monitored removes their reasonable expectation of privacy—the element that often forms the basis for invasion-of-privacy lawsuits arising under common law.

And while being transparent about the use of such monitoring tools is essential to avoiding legal pitfalls, it's also key to building trust in the workforce around privacy issues.

According to a June study by Gartner, 26 percent of HR leaders report having used some form of software or technology to track remote workers since the start of

Many executives are eyeing the use of such technology because they understand that remote work is here to stay.

the coronavirus pandemic. That's up from 16 percent in April, when the pandemic was taking hold. The tracking includes monitoring of work computer usage, employee emails or internal communications, work phone usage, and employee location or movement.

Many executives are eyeing the use of such technology because they understand that remote work is here to stay. Gartner projected that 47 percent of employers plan to let workers work remotely full time moving forward. In addition, 82 percent of business leaders across multiple industries plan to allow employees to work remotely at least some of the time as they reopen closed workplaces.

It's important for organizations to be clear about their intentions when using employee monitoring tools, says Josh Bersin, HR industry analyst and founder of the Josh Bersin Academy in Oakland, California, a professional development organization for HR.

"Is the purpose to benefit employees, to evaluate them, or perhaps to penalize them?" Bersin says. "If the idea is to benefit employees, it's good; if it's to evaluate employees, it's potentially dangerous; and if it's to penalize them, it's probably a bad idea."

MULTIPLE MONITORING TOOLS

Companies such as Teramind, ActivTrak, InterGuard, Sneek, and Hubstaff offer technologies that enable organizations to monitor their employees at home. "These are tools that many companies weren't buying before," says Brian Kropp, chief of research in the HR practice at Gartner.

Teramind's technology can track employee time spent on apps, websites, or email; gauge team productivity levels; and help enforce data security policies. Teramind has seen three times the normal amount of sales leads arriving to its website since the start of the COVID-19 crisis, says Eli Sutton, vice president of global operations for the Miami-based company.

Teramind's tool gives workers an option to periodically log out of the monitoring software to briefly complete nonwork tasks, such as checking personal email.

One way organizations use the technology is to track the time remote employees spend in productive versus unproductive or "nonwork-related" applications or websites, Sutton says. The tools have the ability to gauge active versus idle time spent in targeted areas.

Teramind's tool gives workers an option to periodically log out of the monitoring software to briefly complete nonwork tasks, such as checking personal email. "It al-

lows them to regain their full privacy, which is well-suited for today's work-at-home environment," Sutton says. The technology also can be automatically disabled if employees access sensitive websites, Sutton says, such as a healthcare portal or a personal bank account.

ActivTrak is another company offering technology that can give HR and line leaders greater visibility into how employees spend their time at home.

"A growing interest of our clients is looking for ways to improve the productivity and work habits of remote employees and teams," says Javier Aldrete, vice president of products for Austin, Texas-based ActivTrak. "The technology also can indicate signs of potential disengagement or burnout, since it provides reports on when and how long employees are working on specific tasks each day."

ActivTrak also helps ensure remote employees are using good data security practices. For example, if workers are saving files to storage areas not authorized by the company or using apps not approved by the organization, automatic alerts can be sent to managers who can follow up on such practices.

LEGAL IMPLICATIONS OF MONITORING

Employers using monitoring technology for remote workers face the same legal guidelines as when using such technology in the workplace, legal experts say. But there are special considerations when employees use personal devices for work purposes at home.

"In most instances state laws require you to protect employees' privacy rights by giving them advance notice of your monitoring," says Jennifer Betts, an employment attorney for Ogletree Deakins in Pittsburgh. "The best practice is to get employees' consent for monitoring in writing."

Such transparency is not only good legal practice but

also good management practice. "We've consistently found that when employees are surprised by the use of monitoring technologies, they get very frustrated" and it impacts their morale, Kropp says. "The word will always get out that these tools are being used, so the question is whether you want employees to learn about it from management or from another source."

When organizations install monitoring technology, they need to consider that remote employees may be using personal devices for work tasks, says Usama Kahf, a partner with law firm Fisher Phillips in Irvine, California.

"We've consistently found that when employees are surprised by the use of monitoring technologies, they get very frustrated."

"Employees generally have an expectation of privacy in their use of personal computers and phones unless a different company policy has been communicated to them in writing," he says. If you're using any form of monitoring technology that affects employees' personal devices and retaining information from that monitoring—beyond information gathered when an employee's device is interacting with a corporate network—there should be a written privacy policy disclosing what the company is doing and why it's doing it, Kahf says.

"That policy should detail those situations and uses where employees won't have a reasonable expectation of privacy," he says.

When an employee's personal device is connected to a corporate network or virtual private network (VPN), Kahf says companies do have a legal right to require employees to agree to data security monitoring measures in those situations.

Legal issues also are arising around the use of videoconferencing to conduct business, Betts says, specifically related to the recording of the images and voices of employees without their permission. Organizations, for example, might use such video recordings to create transcripts or to document calls or for future training purposes.

"Some states have wiretapping laws that restrict employers from recording their employees' voices or images without their consent," Betts says.

FORWARD-THINKING USES OF MONITORING

Some organizations are using the data they gather from monitoring not only to keep tabs on remote employees but also to help plan for an eventual return to the workplace.

Kropp says one financial services company measures the performance of its front-line employees in two key ways: the number of insurance claims they process in an hour and the error rate associated with those claims. As the company analyzed the performance of remote workers during COVID-19, it discovered something of interest: Various employees were operating at peak productivity and efficiency levels at very different times of the day.

"They found that some people had a faster claims-processing speed and lower error rate earlier in the morning and others performed better on those metrics in the afternoon," Kropp says. "Some also were doing their best work later at night."

He says such findings may prove useful as the company begins to transition employees back to the workplace. "Many organizations will have to do social distancing in the workplace, and they may 'time shift' when employees work," he says. "To the extent they can schedule worker

shifts when people have proven to be their most productive at home may be beneficial."

Whether business leaders are anticipating a return to the office, a fully remote workforce or something in between, monitoring tools can provide valuable insights into how work gets done and how organizations can support their frontline workers.

WHEN MONITORING, KNOW YOUR OBJECTIVE

Business leaders have a wealth of technology options to choose from when monitoring the activities of remote employees. Experts say the decision on what type of software to use—or even to monitor at all—comes down to a few fundamental questions: Why are you tracking your work-

But he encourages other organizations to use monitoring software with the idea of gaining a deeper understanding of the behaviors and challenges of remote workers, not to keep eyes on their every keyboard stroke.

ers? Is your primary motivation improving the productivity and working conditions of your remote workforce? Or are you applying greater oversight and policing to ensure work-at-home time isn't abused?

While some technologies can address both goals, it's important to be clear about your objectives, says David Johnson, an analyst with Forrester who specializes in workforce productivity issues. On its own, the knowledge of being watched usually improves human behavior, experts say. But when used in draconian fashion, surveillance can damage worker trust and reduce employees' willingness to go the extra mile for their organizations.

Some companies in heavily regulated industries, such as finance or healthcare, may have a need to monitor workers for compliance reasons, Johnson says. But he encourages other organizations to use monitoring software with the idea of gaining a deeper understanding of the behaviors and challenges of remote workers, not to keep eyes on their every keyboard stroke.

"The software can give you good insight into how people are spending their time at home and whether they might have too much or too little on their plates," Johnson says.

Companies that excel at creating a good employee experience look at the data created by monitoring software from a place of curiosity, not punishment.

"The primary goal of a leadership team should be figuring out how to support the needs of their remote workforce. That might require changes like more automation or better technical support. Companies that excel at creating a good employee experience look at the data created by monitoring software from a place of curiosity, not punishment."

KNOW WHAT'S BEING MEASURED

While monitoring software can gauge how often remote employees use work-related applications such as email, Word, Excel, or PowerPoint—as opposed to time spent on nonwork websites or apps—those metrics can sometimes be deceptive.

"Trying to draw conclusions about people's productivity from software use can be a slippery slope," Johnson says. "Does more activity mean that employees are being more productive? Not necessarily, especially where it involves knowledge work."

The highest-performing, most productive employees don't always log the longest hours, Johnson says. "Top employees might work fewer hours in a day but are far more efficient and effective in how they use that time."

TRANSPARENCY AND INTENT

Transparency is key to effective use of monitoring software.

"If employees aren't told they're being monitored by management but find out in another way, it becomes highly uncomfortable," says Stacey Harris, chief research officer for Sapient Insights Group, an Atlanta-based HR technology research and advisory firm. "You not only need to be transparent about the technology's use, but employees also should know why they're being monitored."

Intent makes all the difference in the use of monitoring tools, Harris believes. "It's very easy to make policy based on the lowest common denominator, or the people who break the rules most in companies," she says. "But the organizations who excel at this make policies not based only on those outliers but on employees who get their jobs done in the most productive fashion, to ensure those people have the support and resources they need to keep performing at the highest levels."

While monitoring software has its place, it shouldn't be viewed as a panacea. "There's no substitute for managers staying in frequent touch with their people, even in remote environments," Johnson says. "That's simply good leadership practice that can't be replaced with a productivity tracking tool."

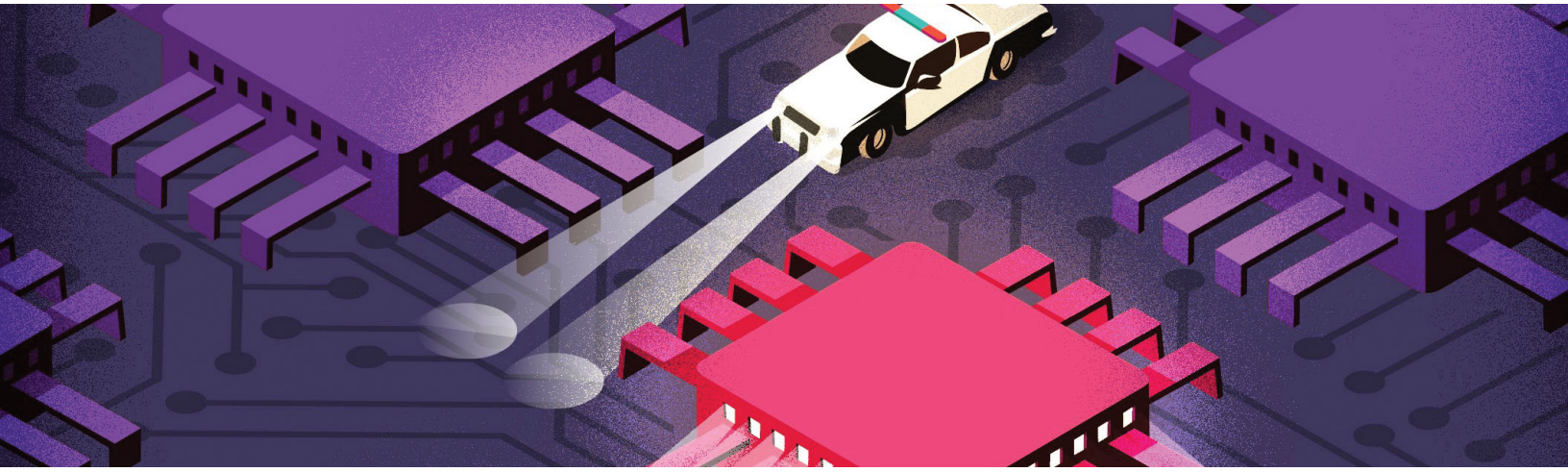
DAVE ZIELINSKI IS A FREELANCE BUSINESS WRITER AND EDITOR IN MINNEAPOLIS.

SECURITY MANAGEMENT

A Patrol Problem

Organizations are getting better at patch management, but they still fail to invest in capabilities to detect and respond—quickly—to data breaches, an annual report finds.

By Megan Gates



The FBI Citizens Academy is a staple of the Bureau's community building initiative. Held over the course of six to eight weeks in cities throughout the United States, FBI agents educate business, religious, civic, and community leaders about how the Bureau investigates crimes and protects public safety.

When John Loveland, global head of cybersecurity strategy and marketing for Verizon, attended the academy, the agent in charge discussed tactics the FBI uses to detect bombers and provide security at large scale events—such as the Boston Marathon. One common approach is placing police cars and officers near major intersections to monitor traffic and identify suspicious activity.

"There was a question in the course of, 'Are you relying

on those metro police officers to detect if there's a truck bomb?'" Loveland says. "The agent's comment was, 'If I have to rely on those guys, I've screwed up.'"

The FBI instead relies on investigative and detection methods that would ideally alert the Bureau to a potential bomber long before he or she went by one of those police officers stationed at a traffic ramp. But this is often not the approach that organizations are taking towards cybersecurity.

"We're spending a lot of time putting cop cars at the entrances to our networks to keep bad guys out, but at the end of the day, the exploits are such that some hackers are going to get through," Loveland says. "Companies have to be spending as much if not more on tech and solutions that help quickly detect when there's an anomaly in the system."

Loveland's assessment is based on findings from the 2020 Verizon Data Breach Incident Report (DBIR), which found

The FBI instead relies on investigative and detection methods that would ideally alert the Bureau to a potential bomber long before he or she went by one of those police officers stationed at a traffic ramp.

that while containment time for a data breach is down to days or less "discovery in months or more still accounts for over a quarter of breaches."

Now in its 13th year, the report has grown to analyze 32,002 security incidents of 157,525 total incidents from data submitted by 81 contributors from 81 countries. Verizon defines incidents as "security events that compromise the integrity, confidentiality, or availability of an information asset."

The report also includes analysis by industry—broken out into 16 verticals—to help practitioners improve their ability

to defend against and mitigate the effects of data breaches (an incident that results in confirmed disclosure of data to an unauthorized party), of which there were a confirmed 3,950 in 2019.

There were a few key themes presented in the data this year. The first was that the use of ransomware continues to grow—representing 20 percent of all malware-related breaches in 2019. Verticals that saw the greater rise in ransomware attacks were against education and state and local governments.

We're spending a lot of time putting cop cars at the entrances to our networks to keep bad guys out.

"We saw a trend in that direction that just really caught fire," Loveland adds. "I venture to say that a majority of the tier 1, tier 2 municipalities have faced some form of ransomware attack."

Ransomware is primarily being introduced to the environment through phishing, which is used to capture user credentials to gain access to Web applications, Loveland says.

This has even greater consequences as the world continues to move towards the cloud and rely on security as a service (SaaS) applications.

"You're expecting [Amazon Web Services] and these platforms to have high level, high grade security to prevent break-ins," Loveland explains. "But a point of vulnerability remains with compromised user credentials. Robust security is possible, but if someone gets ahold of your or my credentials and uses it to access the system—all those defenses are for naught."

And the individuals often behind these breaches are external actors (70 percent) typically associated with

organized criminal groups (55 percent of breaches). Most of these breaches were carried out for financial gain (86 percent) and were discovered in days or less (81 percent).

"One thing that gets press attention is nation-state actors looking for intellectual property—that's stolen or used for competitive advantage," Loveland says. "That occurs in manufacturing and the public sector, but by and large these breaches are financial in nature."

Loveland also explains that breaches are perpetrated by insiders, but that does not always mean the insider is acting maliciously. Many of these breaches are the result of errors or misconfigurations in systems that inadvertently cause a data breach.

"...in spite of what you may have heard through the grapevine, external attackers are considerably more common in our data than are internal attackers, and always have been," according to the report. "This is actually an intuitive finding, as regardless of how many people there may be in a given organization, there are always more people outside it. Nevertheless, it is a widely held opinion that insiders are the biggest threat to an organization's security, but one that we believe to be erroneous. Admittedly, there is a distinct rise in internal actors in the data set these past few years, but that is more likely to be an artifact of increased reporting of internal errors rather than evidence of actual malice from internal actors."

The report's authors saw this most frequently in the healthcare vertical, where internal actors were responsible for approximately 50 percent of breaches. This is because they are working in a "fast-paced environment where a huge amount of work must be done and is also facilitated by paper," Loveland says. "They often don't have controls that are up to snuff—leaving lots of room for errors."

Errors have always been common in industries with

mandatory reporting requirements—like public administration and healthcare—but are now rising in other industries, too.

"The fact that we now see error becoming more apparent in other industries could mean we are getting better at admitting our mistakes rather than trying to simply sweep them under the rug," according to the report. "Of course, it could also mean that since so many of them are caught by

External attackers are considerably more common in our data than are internal attackers.

security researchers and third parties, the victims have no choice but to utter 'mea culpa.'"

In fact, security researchers were the individuals most likely to alert organizations of a data breach—notifying organizations roughly 50 percent of the time, six times higher than in 2018. Less than 10 percent of breaches were reported by internal employees.

This demonstrates the gap that continues to exist in organizations' ability to detect when they have experienced a breach and that the focus on perimeter protection—instead of detection and response—is misguided.

For instance, organizations should be looking to enhance their detection and response capabilities by creating more points to monitor movement through their network and on devices. These measures are also imperative given the rise of remote work in response to the coronavirus pandemic.

"How are companies extending the security fabric outside their four walls?" Loveland asks. "How do you install that same behavior and vigilance at home that you have in the office?"

One positive finding from the data, Loveland adds, is that there has been a steady decline in vulnerability exploits being used to compromise organizations. A common example of this tactic is the Equifax breach, where a Web application was compromised because the company failed to patch a known security flaw.

"We're seeing patching and patch management start to have an impact in reducing some of the vulnerability exploits and also reducing things like Trojans," Loveland says. "Hygiene is on the increase; it's helping reduce those traditional attacks."

SECURITY MANAGEMENT

The Faults in 5G

As the world prepares for the final rollout of 5G, some nations are more prepared to address vulnerabilities than others.

By Megan Gates

Joined by then Forrester Research Vice President and Principal Analyst John Kindervag, the Zero Trust approach means instead of trusting that all users have not been compromised and are acting normally, network owners and operators assume that no user can be trusted and that their actions need to be verified.

This philosophy is gaining greater appreciation as the world rapidly deploys the fifth generation (5G) of wireless technology, capable of peak data rates of 10 gigabits per second. More than 225 cities worldwide have already deployed 5G networks. By 2020, Verizon estimates that 5G will support the connection of more than 20.4 billion Internet of Things (IoT) devices.

This new network structure will allow more devices to be

connected to each other and transfer data at faster speeds than society has seen before. But what happens if the infrastructure used to support these networks is compromised?

To find out, the European Commission conducted a risk assessment of the cybersecurity of 5G networks. It asked EU member states to answer a questionnaire and then published the findings in a report released in October 2019 (EU coordinated risk assessment of the cybersecurity of 5G networks).

The report found that the rollout of 5G networks will create an increased exposure to cyberattacks and more potential entry points for attackers.

"With 5G networks increasingly based on software, risks related to major security flaws, such as those deriving from poor software development processes within suppliers, are gaining in importance," the commission said. "They could also make it easier for threat actors to maliciously insert backdoors into products and make them harder to detect."

The report also highlighted threat scenarios targeting 5G that would have major ramifications if they were carried out: network disruption, spying on traffic or data in the network, modification or rerouting of traffic or data in the network, and destruction or alteration of other infrastructure and systems connected to 5G networks.

"An important difference compared with threats to existing networks concerns the nature and intensity of potential impacts of threats," the risk analysis found. "In particular, greater reliance on economic and societal functions on 5G networks could significantly worsen the potential negative consequences of disruptions. As such, the integrity and availability of those networks will become major concerns, on top of the existing confidentiality and privacy requirements."

The risk assessment also found that the threat posed by

nation-states, or nation-state backed actors, is the highest relevant threat to 5G networks.

"They represent the most serious, as well as the most likely threat actors, as they can have the motivation, intent, and most importantly the capability to conduct persistent and sophisticated attacks on the security of 5G networks," according to the assessment.

This finding is especially concerning for the security community because China has made a strategic investment in 5G. Chinese company Huawei is a major player and has built a vast 5G network that supports activity in the European Union, the United Kingdom, and the United States, despite recently being blacklisted by the Americans.

The overall goal is to enhance the service available at the facility and increase pedestrian access to the building beyond the typical 8 a.m.–5 p.m. business hours.

"The European Commission's report makes clear that the vulnerabilities facing a Huawei 5G global network are systemic," says Nate Snyder, former Obama administration senior counterterrorism official with the U.S. Department of Homeland Security and Countering Violent Extremism Task Force. "Huawei's networks are a house of cards supported by shoddy coding and a supply chain full of holes, with countless entry points for state and non-state actors, organized crime, and terrorist groups—cyber-based and otherwise—to exploit."

To mitigate the risk of attacks exploiting these vulnerabilities, Snyder says the European Union and United States need to focus on creating their own interoperable standards, diversifying their supply chains, and working with stakeholders to build a "stronger foundation and protocols

for the world to jump on the 5G highway."

These efforts were the focus of a recent U.S. Senate Homeland Security and Government Affairs Committee hearing where stakeholders discussed the recent "rip and replace" mandate for Huawei's equipment, increasing U.S. investment into the deployment of 5G, and addressing network insecurity.

"We need to start thinking about investing in technologies that allow us to be secure when we connect to insecure networks," said Jessica Rosenworcel, U.S. Federal Communications Commission (FCC) commissioner.

In her testimony, she referenced the Defense Innovation Board—a U.S. military advisory board of academic researchers and private sector technologists—which found that the nation that owns 5G will own innovations and set standards for the rest of the world. The United States is not immediately poised to be that nation, Rosenworcel explained, and that needs to change through strategic rollout of a national plan for 5G that addresses both infrastructure and device security.

"We need to adjust our policies now to ensure this future is secure," she said. "After all, the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks." ◪

MEGAN GATES IS EDITOR-IN-CHIEF OF SECURITY TECHNOLOGY. CONTACT HER AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.

SECURITY MANAGEMENT

Flight Risks

End users are increasingly adopting unmanned aerial systems for security and operational needs. But they could be introducing cybersecurity risks in flight.

By Megan Gates

It starts out as an idea with the best intentions. Britain's bee population is collapsing, so a private company strikes a deal with the government to provide minuscule robotic drones to pollinate plants and save the nation's agriculture—and humanity itself.

But this good idea in "Hated in the Nation"—a buzzy episode in the science fiction anthology TV series Black Mirror—soon devolves into unintended consequences. The drone bees' source code can be compromised, and instead of simply spreading pollen from plant to plant, they begin to target and kill humans who engage in public shaming on social media using the hashtag #DeathTo.

While fantastical, the episode points out the dangers of using tools without understanding their vulnerabilities.

Drones, or unmanned aerial systems (UAS), have become increasingly used operational tools over the past several years. Goldman Sachs predicted that by 2020, there would be a $100 billion market opportunity for drones, with high demand from the commercial and civil government sectors.

"Drones are already generating climate data, monitoring the borders, and more—and they're just scratching the surface of their commercial potential," Goldman Sachs said in an industry insights report.

The U.S. Department of Interior (DOI) is one of these users, with a fleet of UAS to meet statutory obligations such as emergency management, fighting wildland fires, conducting search and rescue, surveying federal land, collecting research data, and assisting law enforcement. It also uses drones to assess, collect, and maintain information on critical infrastructure, including energy, transportation, and defense-related systems.

In January 2020, U.S. Secretary of the Interior David Bernhardt signed an order grounding all of the department's nonemergency unmanned aircraft systems fleet operations.

"Drones are important to critical Department of the Interior missions, such as combating wildfires and conducting life-saving search and rescue operations; however, we must ensure that the technology used for these operations is such that it will not compromise our national security interests," said DOI spokesperson Carol Danko. Drone operations could continue, however, for fighting wildfires, search and rescue, and dealing with natural disasters that threaten life or property.

Bernhardt issued the order during an internal review of the department's drone fleet's cybersecurity, technology, and domestic production concerns. In a follow-up with Security Management, DOI spokesperson Conner Swan-

son says that Bernhardt received classified briefings on security concerns related to the department's drone fleet in late 2019.

"Currently, we are working hand-in-hand with experts in the executive branch to coordinate a thorough assessment of certain DOI drones and scanning for any potential national security threats," Swanson explains. "This thorough review will ensure that a robust, secure, and reliable source of unmanned aerial systems is available to meet DOI's multiple needs."

Swanson did not say what specific threats the DOI was examining or confirm when the department would complete its review. He also did not elaborate on whether

We find that nearly all DHS components and offices could become victims of a drone-led botnet or data exfiltration attack.

the department had guidance for the public and private sectors, which could be using drone systems similar to the department's to carry out operational surveillance and inspections.

The decision, however, was seen by some as a political maneuver by the Trump Administration to target Chinese drone manufacturers, like DJI Technology, which supplies approximately 20 percent of DOI's grounded drone fleet.

In a statement released shortly after the DOI order, DJI said it was "troubled" by the secretary's order that essentially prohibits employees from operating drones made by foreign-owned companies or those made with foreign-manufactured components based on "undefined cybersecurity concerns."

Prior to the order, DJI worked with the department, cyber-

security professionals, and NASA officials to create a drone solution that met DOI's security requirements.

"The result of this collaboration was our Government Edition (GE) solution, which provides additional safeguards, so drone data is not intentionally or accidentally stored with unauthorized parties," DJI said. "Just a few months later, at the request of the Department of Homeland Security, our GE drones were independently evaluated a second time by the Department of Energy's Idaho National Lab, which also found no areas of concern related to drone leakage."

DJI has worked to increase the security features on its drones, even those not used by the U.S. federal government, says Michael Oldenberg, DJI's senior communications manager for North America.

One feature is local data mode, which allows drone users to eliminate the connection and data transfer between the drone operator's mobile device (connected to the drone) and DJI's servers.

"We developed that for customers doing critical infrastructure inspection as an added assurance that no data is leaving that mobile device while they're using the DJI app," Oldenberg explains.

DJI also offers to host flight data on server infrastructure hosted by Amazon's AWS and the Alibaba Cloud in the United States for its customers outside of mainland China. Customers can use this option to upload the GPS paths of drone flights, along with thumbnails of images taken while the drone is in flight.

Oldenberg says some customers are interested in having this option for auditing and compliance reasons. For instance, a utility operator could use the saved data to show an auditor that an inspector conducted a specific flight path. And any data that is stored on DJI-controlled servers is not synchronized or sent to other

third-party companies. Users who want to delete any data DJI has stored for them can contact DJI to set that in motion, according to a recent white paper on the company's security policies.

Oldenberg says DJI takes users' data security concerns seriously and that the DOI ban is the result of the ongoing geopolitical trade war between the United States and China.

"It has nothing to do with the security or performance of DJI's drones—or any drone manufactured in China," he adds.

However, cybersecurity concerns related to the use of commercially available drones remain. A recent analysis by the RAND Corporation of the U.S. Depart-

My advice to people is to really understand your goal: What are you trying to accomplish using an unmanned system?

ment of Homeland Security's (DHS) use of drones found that the department is vulnerable to drone-enabled cyberattacks.

"We find that nearly all DHS components and offices could become victims of a drone-led botnet or data exfiltration attack," according to the report, How to Analyze the Cyber Threat from Drones. "These offices and components all have physical locations where sensitive data and wireless networks are prevalent, making them targets for these types of attacks. UAS that have loitering capabilities—for example, those that can land and takeoff again after some period of time—allow this type of covert attack, increasing risk to unhardened systems."

Future attack methods could also target DHS employees' personal devices or home networks to gain entry to DHS

systems "either wirelessly or by an employee connecting an infected device to a DHS laptop," the report's authors cautioned.

To mitigate against threats, the authors said DHS needs to develop a coherent UAS cyber strategy—in partnership with senior policymakers, cybersecurity experts, and other government and law enforcement agencies.

"DHS should invest in operating a UAS test range (or ranges) in collaboration with the private sector, national labs, and other government stakeholders such as the Federal Aviation Administration," the report explained. "This step would help ensure industry compliance with safety and security protocols, and would promote interagency coordination."

The report also recommended DHS prioritize the most critical vulnerabilities and find ways to mitigate them, including monitoring developments in counter-UAS systems.

"A coordinated and updateable system of monitoring and intervention is likely to be required as the innovation cycle of cyberattack and countermeasure ensures that even hardened systems cannot be guaranteed immune to attack," the authors wrote.

Additionally, DHS will need to monitor UAS adoption and anticipate how this will affect its security posture.

"As UAS are used in a wider range of activities, the number of legitimate-use UAS that are airborne at any given time will increase," according to the report. "From the perspective of threat mitigation, one of the most important tasks in this new UAS-dense environment will be distinguishing licit from illicit activity."

As of Security Management's press time, the DOI had not issued findings from its review. Regardless, nongovernment users should be thinking about the security of their drone systems and their level of exposure, says James Acevedo,

CPP, founder of StarRiver Inc., who specializes in drone security and regularly builds his own.

Acevedo first raised concerns about drones that were manufactured in China and the need for greater cybersecurity protections at the 2014 ASIS Seminar and Exhibits (now GSX) in Atlanta. His biggest concern at the time was that these drones were designed to be connected to smartphones. Because of their connection to the Internet, Acevedo says users could unknowingly be uploading more flight data and sensitive information than they intended to—creating a security risk.

"My advice to people is to really understand your goal: What are you trying to accomplish using an unmanned system? What's the goal?" he says. Once users have their purpose for the system determined, they can consider where the drone is manufactured, what kind of data it aggregates, and their ability to access that data and delete it.

"People are going to these drones like the ones made by DJI because they're user friendly and intuitive," Acevedo says. "But there are risks attached to it. You should conduct a risk assessment, and if you're willing to accept that risk—fine. But realize that your system could be compromised at some point in time."

SECURITY
MANAGEMENT

ASIS INTERNATIONAL
Advancing Security Worldwide®

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals. *Security Management* is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.

To join ASIS International and become a subscriber to *Security Management*, visit asisonline.org/membership/join.

ASIS INTERNATIONAL

COVER YOUR BASES

ASIS membership has you covered. From thwarting threats to unlocking new career opportunities, ASIS membership will keep you ready for what's next, no matter what the future holds.

Check all the boxes – Join ASIS

asisonline.org/join