141 Cybersecurity Predictions For 202(

Gil Press Contributor ⓘ
Enterprise & Cloud
I write about technology, entrepreneurs and innovation.

Serial cybersecurity entrepreneur Shlomo Kramer said in a 2005 interview that cybersecurity is "a bit like Alice in Wonderland" where you run as fast as you can only t stay in place. In 2020, to paraphrase the second part of the Red Queen's observation (actually from *Through the Looking Glass*), if you wish to stay ahead of cyber criminals you must run twice—or ten times—as fast as that.

The 141 predictions listed here reveal the state-of-mind of key participants in the cybersecurity defense industry and highlight all that's hot today. The future is murky, but we know for sure that on January 1, 2020, the California Consumer Privacy Act (CCPA) will go into effect; that the U.S. presidential election will take place on November 3, 2020; and that on October 1, 2020, if you "wish to fly on commercial aircrafts or access federal facilities" in the U.S., you must have a REAL ID compliant card.

Other than these known events, the crystal balls of the participants in this survey warn us about the impact of emerging technologies such as AI, 5G, and quantum computing and evolving technologies such as the internet of things (IoT), things that move (autonomous vehicles and mobile phones), and the cloud; the role cybersecurity will play in the presidential election; the emerging global cyber war; the increasingly targeted and profitable ransomware attacks; the sorry state of personal data privacy; th significant issue of the best way to deal with identity and authentication; the new targe and types of cyber attacks; how to fix cyber defense; the important role people play in cybersecurity and the what do about the cybersecurity skills shortage; and the good, th bad, and the ugly of the business of cybersecurity.

To win a war, you better join forces with like-minded allies, something that unfortunately may not be considered at all by the entities under attack, but has proven to be a successful strategy for cyber criminals. “It takes a network to defeat a network” says Rina Shainski, Co-Founder and Chairwoman of Duality Technologies.

141 predictions for 2020 from key participants in the cybersecurity defense industry, highlighting ... [+] GETTY

What role emerging technologies (AI, machine learning, 5G, quantum computing) and evolving technologies (IoT, mobile—including autonomou vehicles, cloud) will play in improving the efficiency and effectiveness, breadth and depth, of cyber attacks in 2020?

“AI is going to be HUGE in 2020. And by huge, I mean that a lot of vendors will claim they are using AI—ranging from using simple linear regressions, up through using deep learning. While linear regression is pretty far from AI, we might trust those vendors more to deliver a working product than many who use deep learning techniques as the entirety of their solution. What we’ll see in many spaces is folks starting to understand *the limitations of algorithmic solutions*, especially where those create, amplify, or ossif

bias in the world; and companies buying technologies will really need to start understanding how that bias impacts their operations"—Andy Ellis, Chief Security Officer, Akamai

"As AI adoption in cybersecurity expands, security concerns around AI bias will grow. A security teams' use of AI continues to grow, they'll need to *monitor and manage for potential bias in their AI models to avoid security blind spots* that result in missed threats or more false positives. One way to help prevent bias within AI is to establish cognitive diversity - diversity in the computer scientists developing the AI model, the data feeding it, and the security teams influencing it"—Aarti Borkar, Vice President, IBM Security

"In the world of financial services, because of the ever-growing number of financial cyber-attacks, *regulators will become more open to banks using advanced AI systems to identify unknown and unexpected threats*. However, explainability and transparenc of these AI systems will be crucial"—Mark Gazit, CEO, ThetaRay

"As the use of AI continues to permeate the business world and influence decision making, there will be increasing scrutiny and attention given to interpretability of AI in order to support organizational adoption of AI solutions. With this, *we will see an increase in legal and technical experts focusing on how to effectively audit AI algorithms for bias*. Human-interpretable models that account for biases such as gend or race will help prevent occurrences such as the recent gender-based Apple Credit Car algorithmic misstep"—Justin Silver, Ph.D., Manager of Data Science & AI Strategist, PROS

"We will see threat actors use deepfakes as a tactic for corporate cyberattacks, similar t how phishing attacks operate. That's where the money is for cyber crooks, and they can wreak serious havoc on unsuspecting employees. This means organizations will need to keep validation technology up-to-date; *the same tools that people use to create deepfakes will be the ones used to detect them, so it'll be an arms race for who can use the technology first*"—Sami Laine, Director of Technology Strategy, Okta

"*We expect deepfakes to make a notable impact across all aspects of our lives in 2020* as their realism and potential increases. We will see Deepfakes-As-A-Service move to tl

fore in 2020 as deepfakes become widely adopted for both fun and malicious reasons"-Audra Simons, Director of Innovation, Forcepoint

"As many have feared, *in 2020 we'll see the first malicious use of Deepfakes and other forms of synthetic media with the aim of influencing the Presidential election*, though these efforts will largely fall flat (though there will be at least one attempt that does initially cause a good deal of outrage). This will be due to a combination of greater awareness by the general public of the need to be more skeptical of video evidence circulating online, combined with publishers and social platforms employing detection tools like Deeptrace to help them identify Deepfakes and blunt their impact"—Peter Rojas, Partner, Betaworks Ventures

"The building blocks are well in place for the rise of AI-powered cyberattacks in 2020, a more sophisticated defenses and access to open-source AI tools incentivize adversaries to supercharge their attacks. AI won't only enable malware to move stealthily across businesses without requiring a human's hands on the keyboard, but attackers will also use AI in other malicious ways, including determining their targets, conducting reconnaissance, and scaling their attacks. *Security experts recognize that defensive AI the only force capable of combating offensive AI attacks* and that the battle must be fought by matching – or exceeding – the speed with which attackers innovate"—Marcu Fowler, Director of Strategic Threat, Darktrace

"AI will take a more prevalent role in malicious actors' attack arsenals. They will be abl to launch unlimited autonomous attacks with a reduced need for human intelligence"– David Schwed, Professor and Founding Director of Cybersecurity Program at Yeshiva University's Katz School

"AI and speech technology will be exploited, making voice a new weapon of choice. We see business email compromise (BEC) extend further over into voice next year. Even though many organizations have educated employees on how to spot potential phishing emails, many aren't ready for voice to do the same as they're very believable and there really aren't many effective, mainstream ways of detecting them. And while these types of "voishing" attacks aren't new, *we'll see more malicious actors leveraging influential voices to execute attacks next year*"—PJ Kirner, Founder and CTO, Illumio

"With advancements in the deepfake voice technology, *I expect a rise of voice phishing schemes in 2020* in which employees are tricked into sending money to scammers or revealing sensitive information after getting voice messages and calls that sound like they are from the CFO or other executives. Given how hard it is to identify these deepfakes compared to standard phishing attacks, I expect these operations will becom the norm in the new year"—Curtis Simpson, CISO, Armis

"Deepfakes and synthetic identities will open the door for the next wave of identity fraud. Fraudsters are gaining access to ever-more sophisticated technologies for creati not just false ID images, but fake data records to back up that false identity. Traditiona identity verification solutions are not equipped to detect these methods, and businesse large and small are at risk. To counteract this threat, companies will need to invest in more sophisticated verification technologies, including AI and machine learning algorithms, as well as staff trained to identify the tiny details that give away these new types of fraud"—Sanjay Gupta, VP & GM of Corporate Development, Mitek

"NIST recently released 'A Taxonomy and Terminology of Adversarial Machine Learning' in draft form in order to standardize the language used in the nascent field of Adversarial Machine Learning. *There are many unknowns for how attackers can manipulate machine learning through training data poisoning or evasion attacks*. It feels a bit like when we were building web applications and didn't know about SQL injection attacks. Processes and methodologies get put into place that don't account for the way AI can be attacked"—Chris Wysopal, Co-Founder and CTO, Veracode

"Hackers will attack AI while it's still learning. As we increasingly depend on smart technology, the door for sabotage keeps opening wider and wider. The training needed to teach smart algorithms will be the perfect place for bad actors to take action against them. Data integrity has never been more important"—Eric Sammer, Distinguished Engineer, Splunk

"Disinformation and fake news can spread havoc in both the public and private sector and is increasingly being used as a weapon by nation states. In 2020, we will see more the terrifying reality that deep learning algorithms can bring about in generating fake, but seemingly realistic images and videos. This application of *AI will be a catalyst for large scale disinformation campaigns that are targeted and individualized to the*

behavioral and psychological profiles of each victim, furthering reach and impact"—Pascal Geenens, Security Researcher, Radware

"As digitization continues in 2020, *data will become more valuable than ever before*. Information that may have previously seemed trivial to the everyday consumer will actually hold significant value for stakeholders and hackers across the spectrum. Adversaries or real-life 'data bounty hunters' will hunt for new ways to exploit it, governments will seek better ways to access it, enterprises will adopt stronger security measures to protect it and end-users will demand better privacy to secure their persona information. Furthermore, with the rise of AI and machine learning, crucial data that impacts how medical decisions are made, where/how autonomous cars move, and mor will become increasingly more mainstream—and increasingly more lucrative to threat actors pining for the information"—Phil Dunkelberger, President and CEO, Nok Nok Labs

"Bots and Robotic Process Automation are hitting the mainstream. No longer the exception, they should be an expected tool in every modern enterprise. Now that they are no longer a surprise, their usage will expand further. This means that new usages fo them will test the boundaries of our current definitions of what they can and should do Over the next year*, I would expect a wave of vulnerabilities and breaches that involve bots*—it is a rich target surface that has not yet been exploited fully. Correspondingly, a they take on more sophistication, regulations will begin to include them and will draw clear lines of responsibility for their human implementers"—Mike Kiser, Global Evangelist, SailPoint

"One of the most significant challenges that IT professionals continue to face is maintaining the environments they are responsible for and ensuring that those environments consistently deliver the business-critical solutions that their organizatior requires. Customers no longer tolerate downtime, let alone data breaches. *In 2020, we see more organizations using AI and predictive proactive management to better anticipate, safeguard and prevent potential threat vectors ahead of time*"—Ken Galvi Senior Product Manager, Quest Software

"With the rapid adoption of Robotic Process Automation (RPA), security has become a afterthought, only being applied once it's too late and regulations are forced on the use

of RPA technology. Like we've seen with other innovations, *there will be a significant breach to RPA technology in 2020,* as this technology will draw attention from cybercriminals who are after the privileged data RPA technologies hold"—Darrell Long Vice President of Product Management, One Identity

"In 2020, there will be a need for adversarial machine learning to combat supply chain corruption. As remote and co-working spaces become more common, a big problem companies will have to face is determining who has access to what data. As a result, *AI will become more prevalent in traditional business processes and be used to identify i a supply chain has been corrupted*"—Sean Tierney, Director of Threat Intelligence, Infoblox

"As cybersecurity threats evolve, *we'll fight AI with AI*. The most successful cyberattacl are executed by highly professional criminal networks that leverage AI and ML to explc vulnerabilities such as user behavior or security gaps to gain access to valuable busines systems and data. All of this makes it extremely hard for IT security organizations to keep up, much less stay ahead of these threats. While an attacker only needs to find on open door in an enterprise's security, the enterprise must race to lock all of the doors. A conducts this at a pace and thoroughness human ability can no longer compete with an businesses will finally take notice in 2020"—Brian Foster, SVP, MobileIron

"Artificial intelligence (AI) and machine learning algorithms used in cybersecurity have historically been trained with Information Technology (IT) network and system behavioral datasets. But in 2020 *we're going to see a rise of AI occurring in Operation Technology (OT) and automation control systems at the edge*, allowing for unprecedented insight into the converging IT and OT ecosystem of smart technologies used in our building environments. *Implementing AI at the edge will provide richer information, allowing us to quickly identify malicious traffic or abnormal behavior* tc further protect our buildings against cyber threats"—Jason Christman, Vice President, Chief Product Security Officer, Johnson Controls

"As the availability and reliability of 5G slowly rolls out, new cybersecurity challenges will emerge as opportunistic hackers look to profit off of the proliferation of IoT data. I the impending 5G enabled world, attack surfaces will be larger than they've ever been before, providing more opportunities for consumers and businesses to be hacked. In

addition, ultra-high bandwidth will empower criminals to launch much larger botnet and DDoS attacks that could cripple entire enterprise networks. *With attackers conducting cyber warfare in 'low and slow' stealth mode, having a granular and comprehensively sufficient data set to detect breeches will be imperative*"—Michael Rezek, VP Cybersecurity Strategy, Accedian

"*What makes 5G a greater-than-normal risk is the high business potential for its use and deployments, which will regularly occur in arguably less-secure industrial environments with outdated, legacy devices*. Adversaries will begin to target these environments, bringing dire consequences such as unauthorized changes to configurations that make industrial processes do something they are not supposed to d thereby, resulting in an industrial accident, outage or even environmental excursion"—Jason Haward-Grau, CISO, PAS Global

"Companies will reach a critical mass of 5G-enabled devices in 2020, forcing them to reevaluate their risk paradigm for connected devices. Further complicating that paradigm is the fact that *devices leveraging 5G could potentially bypass some traditional cybersecurity technologies by connecting directly to cellular networks*. It's unclear if this changing risk paradigm will result in an attack or breach in 2020 due to the newness of the technology, but regardless, companies will have to consider changin their security strategies or leave a growing section of their devices without adequate protection"—Pedro Abreu, Chief Strategy and Product Officer, Forescout

"2020 will be the year of 5G, bringing with it not only faster speeds and bandwidth capabilities to our mobile devices, but also making them highly coveted targets by DDo attackers. While mobile devices have always been targeted by financial or personal data thieves, 5G's increased bandwidth allows attackers to take control over a relatively sma number of mobile handsets and unleash a tremendous amount of damage. A potential DDoS attack may be distributed via an innocent-looking app on the Play or App store and an attacker just needs a few hundred installs to create a massive outbreak"—Hagai Shapira, Research Team Lead, SAM

"The National Institute of Standards and Technology is already researching methods to deal with the effects of quantum power, and for good reason: *hackers may access quantum computers as they become commercial*. Quantum computers can launch

attacks that break asymmetric cryptography, rendering the entire encryption method based on PKI obsolete. As threats become capable of defeating a higher proportion of security efforts, cybersecurity in 2020 will be defined by the need to stand out. Cybersecurity companies will need to take more risks"—Shimrit Tzur-David, Co-Founder and CTO, Secret Double Octopus

"As quantum computers continue to improve, enterprises and the general public will become increasingly aware of the threat they pose to the cryptographic systems that underpin all digital security globally. *We will see a greater focus on crypto agility, or the ability to update cryptographic algorithms, keys and certificates quickly* in response to advances in cracking techniques and processing speed. To prepare for thes inevitable cryptographic updates, more enterprises than ever will explore automation a a critical component for ensuring future-proofed security"—Tim Callan, Senior Fellow, Sectigo

"*Quantum computers will advance far quicker than predicted, leaving enterprises scrambling to become quantum safe*. By the end of 2020 it will be evident that RSA 2048 will be doomed in under 5 years when a nation state like China or the U.S. will have a quantum computer capable of decrypting current encryption paradigms"—John Prisco, President & CEO, Quantum Xchange

"As the IT world has progressed to multilayered security, effectively combining cloud, endpoint, and network protection, the future of IoT cybersecurity is expected to evolve just as quickly, and for good reason given that by 2020, *75 billion IoT devices are expected to be in use and a quarter of cyber-attacks on enterprises will involve IoT devices*. The distribution of billions of vulnerable IoT devices, all of which are highly diverse and tend to have limited resources, significantly increases the attack surface an makes traditional security solutions ineffective. Identifying and addressing the risks of and exposure to hackers seeking to exploit vulnerabilities in IoT devices and applying holistic, endpoint security solutions by manufacturers and enterprises will be key to th future of IoT cybersecurity"—Natali Tshuva, Founder and CEO, Sternum

"The adoption of 5G will enable a massive increase in connected devices. With this influx of IoT devices like sensors, monitors and data collectors *our global data volume will rapidly increase*. With this the need to protect these networks and the sensitive

data that resides on them will require a more focused approach to IoT security"—Jason Albuquerque, CISO/CIO, Carousel Industries Inc

"As we move into 2020, *companies need to shift to a more preventative approach to cybersecurity over a detection-focused approach*. The number of connected IoT device will continue to increase making the likelihood of a cyberattack even more prevalent. The ability to manage and enforce cybersecurity policies for IoT devices prior to an attack rather than in response to one has the potential to mitigate the impact of a cyberattack or even stop it all together"—Wayne Dorris, CISSP, Business Development Manager, Cybersecurity, Axis Communications, Inc.

"In 2020, widespread transformation will become a necessity as *organizations will nee to build security into IoT devices and applications rather than bolting it on to existing technology*. Repercussions of not prioritizing this will become dire as connected device evolve from seemingly trivial tools such as thermostats and refrigerators towards highe stake technology such as autonomous vehicles and more. Without building security int these environments, organizations will put end-users' physical safety, privacy and more at risk"—Sean Peasley, Internet of Things (IoT) Security leader in Cyber Risk Services, Deloitte Cyber

"With the continued developments in IoT and 5G, increasingly more common-use devices will be connected to the Internet, from light bulbs to vehicles. *This will give ris to new forms of security intrusions as well as privacy challenges for both organizations and people*. Companies need to figure out innovative ways to counter them before the harm is done. 2020 will bring some changes in the way organizations think about and deal with both the privacy policies and with their usually understaffed cybersecurity teams"—Lucas Roh, CEO, Bigstep

"*5G will result in the first public disclosure of a data breach caused by a mobile device* Extremely fast 5G connectivity will enable new capabilities for self-driving cars, remote robotic surgeries, and many other applications that require decisions to be made in single-digit milliseconds. However, it will also accelerate the amount of data lost on mobile devices. 5G will continue to dissolve traditional enterprise network perimeters and cybercriminals will take advantage of security gaps to launch all kinds of attacks,

such as phishing, man-in-the-middle, device takeovers, and more"—Brian Foster, SVP, MobileIron

"Automotive OEMs will increase investment in Vehicle Security Operations Centers (VSOC) to monitor connected fleets for cyberattacks. Besides monitoring the mobile applications connected to the vehicles, the VSOCs will add capabilities to monitor the i vehicle network to extend their intrusion detection capabilities. OEMs will also elevate their attention from only protecting the safety systems of vehicles to also defending the monetary software assets in the vehicle, which will require more advanced and more sophisticated cybersecurity solutions"—Yossi Vardi, Co-Founder and CEO, SafeRide Technologies

"In 2020, consumers will suffer from increased 'mobile leeching' attacks. This is an attack aimed at continuously harvesting data, connections, resources and infrastructur from mobile businesses. Leeching can be carried out locally (i.e., on the device itself), where the target is a single user. Leeching can also be carried out against the backend (on PCs or servers connecting to the backend), where the target is the mobile business"—Tom Tovar, CEO, AppDome

"In 2020, the threat from state and state-sponsored APT groups leveraging mobile malware combined with traditional desktop malware in cross-platform campaigns targeting individuals and organizations will become a greater issue. The confidence placed in mobile app store security and overall low mobile threat detection rates have instilled a false sense of security, leaving mobile users an easy target and a significant attack vector for organizations, especially those who allow employees to use their personal devices to access their networks. Enterprises and governments would be wise to consider investing more resources into mobile threat detection and response as part of their overall security strategy moving forward"—Brian Robison, Chief Evangelist, BlackBerry Cylance

"You're only as strong as your weakest link. I would expect a continued growth in the number of attacks that originate through cellular endpoints, which in turn will shift the focus of CISOs to cellular cyber security"—Professor Dror Fixler, Founder and CEO, FirstPoint

"*Cloud jacking and subsequent island hopping will become a more common practice a* attackers look to leverage an organization's infrastructure and brand against itself"—Tom Kellermann, Chief Cybersecurity Officer, VMware Carbon Black

"In 2020,we will begin to see the first (of potentially many) attacks against commercial cloud infrastructure by *exploiting virtual machines and corrupting hypervisors to gai access to other clients' sensitive data*"—Robert Y. Bigman, former CISO, CIA

"*In 2020, the term 'Shared Responsibility Model' will be omnipresent* as everyone will gain its encyclopaedic understanding and realize how important this is. Take for instance the millions of AWS or Azure customers who depend on these services every day—suppose if one day AWS just disappeared and entire businesses would effectively be taken offline? Amazon's likely response would be 'Sorry, here are a bunch of service credits'"—Tal Klein, CMO, Rezilion

"In 2020 and beyond, we anticipate that an increased number of data breaches will result from organizations making the false assumption that cloud service providers offe complete protection, which simply isn't true under the shared reasonability model. As a result, *organizations will fail to identify the gaps that must be addressed within their cloud infrastructure*. Organizations will find themselves liable for loftier repercussions as government cyber-legislation ascribes harsher consequences"—Balaji Parimi, founde and CEO, CloudKnox

"Office 365 is a major target for IP theft, data leakage, credential cracking, and O365-specific attacks because that's where a big bulk of sensitive, enterprise data is. Yet, O36 security issues often don't get the attention they deserve. In 2020 and beyond, *IT shou expect new O365 phishing and malware attacks*, as well as modified versions of KnockKnock and ShurtLOckr, two attacks that focus on Office 365 that have been activ since May 2017—and are still running"—Michael Morrison, CEO, CoreView

"*Security will become a leading decision criterion for the purchase of cloud services*. I will no longer just be about cost, flexibility, tooling and support. As more companies migrate their infrastructure and services to the cloud, we will continue to see a growing emphasis on cloud being a risk"—Tim Chen, CEO, DomainTools

Will rising geo-political tensions translate into a global cyber war in 2020?

"As a show of support for the strife in Hong Kong, well-meaning cyber vigilantes will turn their sights to China and attempt to breach Chinese companies or the Great Firewall, likely leading to major outages for the country. While these efforts are well-intentioned, they may result in unforeseen damages to China's infrastructure, as well a harm to everyday citizens accidentally caught in the crossfire. *With these rising geo-political tensions in mind, visibility into East-West traffic will be more important tha ever to protect the innocent*"—Richard Henderson, Head of Global Threat Intelligence, Lastline

"*Expect to see more attacks against less developed nations*. Attacks like this don't generate revenue, rather they are meant to disrupt and destroy"—Grayson Milbourne, Security intelligence Director, Webroot

"In 2020, a foreign adversary will take advantage of the neglected infrastructure and create *the first monumental disruption in a Western government's electrical grid*. When citizens riot due to the sustained outage, law enforcement will be called to quell the physical disruption as it hurries to fix the electrical one. This will force virtually all large enterprises to have some type of cyber insurance policy in the coming year, and it will focus them on modeling catastrophic cyber incidents surrounding third-, fourth- and fifth-party risk, supply chain disruption, and financial losses"—Jake Olcott, VP, BitSight

"The geopolitical landscape will drastically shift as nation-states gradually increase their use of AI, using complex, sophisticated malware to attack one another's infrastructure. What we'll see is severe damage to a city's or country's economy, power plants, transportation systems and more"—Guy Caspi, CEO, Deep Instinct

"W*e'll see state-sponsored attacks being carried out much more often, possibly even against critical infrastructure*. There have been many attempts and even successful attacks against these types of systems, but most have been isolated incidents. One can only wonder though if these attacks to date were merely conducted to set up backdoor functionality for a future panic button push to cripple the target's systems"—Tim Bandos, Vice President of Cybersecurity, Digital Guardian

"With the continuing escalation of the global trade wars, cyber-attacks will increase and be used to strengthen global influence. Some have coined this the "Cyber Cold War". In the fight for global dominance, cyber espionage and disruption will be increasingly used by global powers, sometimes using smaller countries as proxies, in the goal of gaining political advantage"—Jason Albuquerque, CISO/CIO, Carousel Industries Inc

Will cybersecurity determine the outcome of the 2020 U.S. presidential elections or will it turn out to be a "Y2K"-like event?

"Though we've seen proof that voting machines can be hacked, adversaries won't spend much time targeting them this election cycle. However, *external threat actors will go after state and local voter databases with the goal of creating havoc*, making it harder for legitimate voters to cast their ballots, triggering voter-fraud alerts and generating doubt in validity of vote counts during the 2020 elections"—Corey Nachreiner, CTO, WatchGuard Technologies

"Bots had a substantial impact on the 2016 presidential election, so there is no doubt they will work to influence the 2020 presidential election as well. Bots will not only work to influence public opinion but will also target the election systems themselves. Local and government agencies will need to be prepared for the multiple threats they present as not only do they pose a huge threat to the swaying people's perceptions of candidate but when structured as a 7-layer DDoS attack they have the ability to take down entire election systems"—Tiffany Olson Kleemann, VP of Bot Management, Imperva

"The combination of a higher percentage of digitally-native, first-time voters; an increased reliance on connected systems for registration, tallying, and voting; and the wide knowledge and sharing of Russia's disinformation playbook from 2016 indicates that *we're in for a wild ride through the 2020 elections*—not just in the U.S., and not just with Russia as a potential aggressor. The good news is, we're already seeing a move in the right direction with the call for vulnerability disclosure programs across government agencies, which would allow whitehat hackers to help surface flaws in election websites and applications in lead up to and through the elections"—Casey Ellis Founder, Chairman and CTO, Bugcrowd

"There are serious issues with the way our election infrastructure works, and fixing it would require legislation requiring threat models, standardization, transparency, pape trails, and better testing. And even if our election systems were perfect, attackers don't target the heart of your defenses—they go after the weakest parts. By and large, they don't break encryption, they steal the key from the user. In this case, *the weakest aspec of our election systems is outside the voting infrastructure*, and will require campaign finance, social media, party primary, and even electoral college reform to fix. So, regardless of the election outcome, I think it is extremely unlikely that there will be any significant improvement in time for the 2024 Presidential election"—Jeff Williams, Co-Founder and CTO, Contrast Security

"*The 2020 presidential election will see more meddling than any election before*. Not only will meddling come from nation-states, but we will see interference from pockets within the United States attempting to manipulate their own election. As the diversity o voting methods increases, the attack surface will increase as external and internal threats loom. It will be critical to protect and restrict access to election materials"—Tim Eades, CEO, vArmour

"For individuals in the US, *2020 will be dominated by election security and how misinformation campaigns from state actors on social media can impact the election*. For the corporate world, 2020 is finally the year the cybersecurity industry realizes tha you can't manage what you do not know about, and the investment in asset discovery and automated configuration management databases will skyrocket"—Jerry Gamblin, principal security engineer, Kenna Security

Ransomware: Will "to pay or not to pay" continue to be an unanswered question in 2020?

"To pay or not to pay, that is the question**:** More than 100 public-sector ransomware attacks have been reported in 2019 so far, compared to 51 reported in 2018. As we head into 2020, ransomware attacks will continue to rise and *the targeting of specific industries, locales and public services will continue*. And we will see more debate on paying versus not paying"—Jon Check, Senior Director of Cyber Protection, Raytheon

"Highly targeted ransom will continue. Next year, *ransom-motivated attackers will more pointedly observe automatic backup solutions* and make attempts to remove and alter the backup data or the task itself"—Eric Klonowski, Manager, Software Development, Webroot

"Ransomware isn't the most pervasive or common threat, it's simply the noisiest. In 2020, attacks will become more targeted and sophisticated. *Hackers will pivot from spray-and-pray tactics. They will instead linger on networks and hone in on the most valuable data to encrypt*. Imagine an attacker that encrypts investor information before a publicly traded bank announces earnings. This is the type of ransomware attack I expect we'll see more of in the coming year, and organizations that can't keep up will continue to get hit"—Brian Vecci, Field CTO, Varonis

"In 2020, *we will see the first bank surrender to ransomware*. The year will also bring many struggles to recover data and service"—Yaniv Valik, VP Product, Cyber and IT Resilience, Continuity Software

"Ransomware will continue to be extremely successful in 2020, especially across healthcare and state and local industries. *For the first time we may unfortunately see an attack that results in death(s) due to critical and timely information being unavailable for a patient in an ICU*. The reason for ransomware and other malware being so easily able to inflict damage is our continued reliance on security tools that chase badness rather than ensuring good. It is impossible to detect all badness with a high degree of confidence by relying on the enumeration of badness approach"—Nir Gaist, Founder and CTO, Nyotron

"In 2020, we will see, at minimum, a 300% increase in RYUK-related ransomware attacks, and *most of those attacks will be focused on U.S. small businesses.* Ransoms on small businesses will jump to $150,000 to $300,000 per event on the low end, causing a spike in U.S. small business bankruptcies and closures. About 2 out of every 10 small businesses attacked will have no choice but to halt operations for financial reasons. Another reason we'll see a spike in attacks on small U.S. businesses is the sheer volume of these businesses running outdated windows servers with known vulnerabilities"—Zohar Pinhasi, CEO, MonsterCloud Cyber Security

"2019 was a great year for cyber crooks successfully targeting municipalities, schools and universities worldwide with ransomware and spear phishing attacks. As these organizations have proven easy targets, *a rise in campaigns is expected in 2020*. Healthcare will also be an attractive sector for hackers due to its high potential gains. However, many in this sector are now investing substantial work and resources to improve their security posture so while attacks will occur, they won't be as successful"–Eyal Aharoni, VP Customer Success and Sales Operations, Cymulate

"As the level of sophistication in ransomware attacks and breaches increases, small companies will realize that they now also have targets on their backs. Breaches are steadily becoming inevitable, and the question will evolve from a matter of if to when. The belief that companies with under 1,500 employees are safe because they're 'too small' for attackers will go out the window. *Cyber concerns for small companies will outpace those by large enterprises for the first time*"—Sam McLane, Chief Technology Services Officer, Arctic Wolf Networks

"I believe that we will hear much more next year about ransomware attacks targeting n only large enterprises but also small and medium businesses. These *small companies are more vulnerable than enterprises as they lack the resources and knowledge to protect themselves*. Cyber security companies who will offer zero-deployment tools especially for cloud-based resources will be the nextgen cyber prevention solutions"—Revital Libfrand, CMO, Odi-x

What will governments do—or will not do—about our privacy? Will privacy finally become a top-level business priority? What are the implications for enterprise data management?

"*Advertisers like Google, Facebook, and Amazon are going to start using more offline data to target consumers*. Google's recent acquisition of Fitbit, in particular, means the tech giant has access to years of fitness data for tens of millions of consumers"—Wayne Coburn, Principal Product Manager, Iterable

"Privacy is the watchword for the data-driven technology industry. *With CCPA coming into effect, expect other US states and countries globally to follow suit*. To keep abreas of the changes, consumer-facing businesses will need to embed privacy related activitie

as a default requirement in their operations with consumer consent being mandatory"-Madhu Therani, CTO & Head of AI, Near

"As the stakes for privacy management become higher and higher from endless breach and increased regulation, like GDPR and CCPA, *we'll see enterprises deploy more effective means of privacy control for their employees' personal devices* (like application-specific security, as opposed to only device-level). This will mitigate privacy invasion for employees and enable tighter vulnerability controls for the enterprise, all the while providing the necessary corporate data and accessibility to end-users via the mobile device of their choice"—John Aisien, CEO, Blue Cedar

"In 2020, organizations will be forced to take much needed steps to be data compliant. Furthermore, *the cost of compliance will significantly increase because of the new dat privacy regulations*. As we witnessed with GDPR in the UK and Europe, there will be two schools of thought around CCPA: acceptance and denial. There are those who proactively join the conversation and others that sit in the 'wait-and-see' camp. Organizations that deploy intelligent data security technology with artificial intelligenc driven systems, will have the best outcomes vs. organizations relying on manual processes"—Tony Pepper, Co-Founder and CEO, Egress

"In 2020, there will be a scramble to get in line with privacy regulation. In the last few years, many US companies sat back and watched as GDPR and other regulations were implemented but now they are seeing their friends get fined and privacy is now important at the board level as they are being held responsible for breaches. As California's new privacy law goes into effect in January and other regulations roll out through 2020, *many companies will be crushed by fines and be forced out of business and it will scare the rest into making privacy a top level priority*"—Rich Chetwynd, Product Manager, OneLogin

"In 2020, governments are going to take an even more active role in cybersecurity through encryption regulation. Governments have been clumsy in their attempts to legislate encryption because that technology has been light years ahead of those that ar supposed to regulate it. Next year, they'll be playing catch-up, and we may see some challenges to our privacy as a result"—Jeff Shiner, CEO, 1Password

"*In 2020, image security and privacy will percolate to become a top cybersecurity concern*, driven by anonymity erosion. Face recognition is an emotional topic: from accuracy failures revealed in London to rejection in San Francisco; from desire for privacy to policing needs; from obligation to protect children and assist drivers to accidental or intentional exposure and disclosure"—Ron Moritz, Venture Partner, Cybersecurity and Enterprise Infrastructure, OurCrowd

"2020 will bring an even stronger need to trace everything you do with your data as GDPR and the newly implemented CCPA are carried out. This will make it more important than ever for companies to *have a clear way to account for every bit of data they house, down to how it was obtained, to protect everyone who touched it*"—Jean-Michel Franco, Senior Director for Governance, Talend

"The backup and archiving of personal data have been deemed the largest area of privacy risk for 70% of organizations. This stat will continue to grow and we'll see improvement in data protection tools across the board, both for discovering what data available, as well as how it can be protected after it's identified. The cheapest control is often ignored—simply don't keep the sensitive data. *Companies cannot leak or lose what they do not have*. While GDPR and CCPA may be onerous for some to deal with, these regulations will continue to force companies throughout 2020 to instill and build processes that can identify, deduplicate, centralize and most importantly eliminate sensitive data generating a major win for all"—Andrew Jaquith, Chief Information Security Officer & GM, Cyber, QOMPLX, Inc.

"It used to be that organizations had to spend millions of dollars on consultants to find out where PII (sensitive) data lived, but today there are a number of data privacy and governance technologies that can bolster security and data practices. *Next year will see an inflection point in organizations finally understanding more about their data*, which will be critical to improving data privacy standards as an industry"—Avon Puri, CIO, Rubrik

"*Companies will rely more on metadata than data to provide insights*. Overzealous data analyses have brought many companies face to face with privacy lawsuits from consumers and governments alike, which in turn has led to even stricter data governance laws. Understandably concerned about making similar mistakes, businesse

will begin turning to metadata for insights in 2020, rather than analyzing actual data. I harvesting data's attributes — including its movement, volume, naming conventions ar other properties — companies will give indications of concerns around accessing PII ar other sensitive information. Metadata lends itself well to data privacy, and with the correct machine learning and artificial intelligence modeling, can still provide critical information to the C-suite such as lead generation changes, third-party data access, potential breaches and more"—Steve Wood, Chief Product Officer, Boomi

"With CCPA coming into effect, expect other US states and countries globally to follow suit. To keep abreast of the changes, *consumer-facing businesses will need to embed privacy related activities as a default requirement in their operations* with consumer consent being mandatory"—Madhu Therani, CTO and Head of AI, Near

"Companies will focus solely on aggregating anonymized information that still produce value. Society is now more than ever aware of the risks of personal information being shared or transferred without permission so *products will be built to anonymize that data but retain the value*"—Shaun Moore, Founder and CEO, Trueface

"The rapid emergence of AI and IoT created an unprecedented flood of data, much of which revolves around the very things that make us who we are. As more and more individuals are confronted with AI in their day to day, from job interviews to McDonald's orders, your digital identity will become as much a part of who you are as your DNA. The problem? What happens when someone owns the thing that makes you you? As CCPA and GDPR further restrict what companies can do with personal data, *2020 will see us redefine what it means to be a person, and with that, rewrite the rule of dealing with data*"—Matthew Halliday, Co-Founder and VP of Product, Incorta

"Companies need to know where and how their resources are stored. They need to take the bare minimum steps necessary to secure data. And *they need to minimize their dat because if you're not using it, you need to get rid of it*. Start utilizing the principles of privacy by design"—Matthew Vernhout, Director of Privacy, 250ok

"By 2022, governments, organizations and individuals will realize their failure to prote 100% of their owned/handled information. They will begin limiting protection down to

the most valuable 25%, while placing the rest into fully/partially open access"—Joseph Feiman, Chief Strategy Officer, WhiteHat Security

"*In 2020, it's likely that we'll see some sort of Federal, broad-sweeping regulation like what the EU did with GDPR*. It will involve consumer privacy, and it will be a mandate from the federal level. This is somewhat dependent on the election outcome, and it may not happen next year, but within the next 2-4 years. As far as individual states go, Nevada has a law already in effect and Maine is close to implementing its own legislation, too. This is top-of-mind for CEOs and boards in the year ahead as foreign nation-states continue their hacking efforts"—Matt Kunkel, CEO, LogicGate

"*Federal privacy legislation is not going to happen in 2020, but look for a serious push in 2021*. There isn't yet a bipartisan push that would be essential to get this passed. The current proposals are too one-sided and don't blend the business and consumer perspectives. Plus, the election cycle and the impeachment inquiries make this unlikely even though this is the type of issue that could provide a nice bipartisan approach and accomplishment in the wake of partisan issues. If companies find CCPA difficult to comply with then that will create momentum for action in 2021"—Bret Cohen, CEO, Ti 1 Cyber

Who are you and why should we give you access? Zero trust, authentication identity

"Zero Trust became popular in 2019, especially in the wake of many breaches occurring from within security perimeters. The next step for Zero Trust is for its usability to match its effectiveness. In 2020, *Zero Trust systems will embrace passwordless multi-factor means*, in order to better guarantee that a pragmatic lack of trust will not interfere with normal system operations"—Raz Rafaeli, CEO, Secret Double Octopus

"The vulnerabilities of knowledge-based verification and multi-factor authentication with SMS and email will lead to account recovery processes adopting remote identity verification processes. Businesses will begin to embrace technology-driven authentication methods like authenticator apps, passwordless logins, and biometrics to ensure accounts—and the businesses and individuals behind them—are protected. This change supports *the zero-trust world in which we live in, where the presentation of*

credentials like a password or token is not sufficient to grant access with any level of assurance"—David Thomas, CEO, Evident ID

Enterprises rarely have a complete handle on who has privileged access, and whether the access rights that people do have are the right ones. Now, with the rise of Zero Trus a new, parallel, concept has emerged in the Privileged Access Management space: Zero Standing Privilege or ZSP. *WIth ZSP, users who need privileged access are granted those rights when they need, and when they're done, the privileged access goes away*. This new Just-in-Time approach to privileged access not only closes compliance and audit gaps, but simplifies security management and reduces the threat of compromised administrator credentials"—Paul Lanzi, Co-Founder and COO, Remediant

"*In 2020, Zero Trust will pervade the internal network, and data privacy and securit concerns will impel the hardening of internal infrastructure to include data encryptio both in-flight and at-rest*. Ultimately, hybrid cloud and multi-cloud architectures will force IT organizations to re-evaluate their concept of the 'internal network' and conside Internet-independent private network alternatives"—Steve Litster, CTO, Markley Grou

"With biometric authentication becoming increasingly popular, *we'll begin to see a lev of unfounded complacency when it comes to security*. While it's true that biometric authentication is more secure than traditional, key-based authentication methods, attackers typically aren't after fingerprints, facial data or retinal scans—they want the access that lies behind secure authentication methods. So, while biometric authentication is a very good way to authenticate a user to a device, organizations must be aware that every time that happens, that biometric data must be encrypted and the assets behind the authentication kept secure. More importantly, the network authentication token that's generated must be protected, otherwise attackers can blaze trail across the network, potentially gaining administrative access and privileged credentials to accomplish their goals, while masquerading as a legitimate, authenticate employee"—Lavi Lazarovitz, Group Research Manager, CyberArk

"*Consumers will continue experiencing the great disappearance of identity*. Previousl consumers' identity was managed through traditional means: a password and usernam login. Now, no one has the time or energy (or patience) to deal with the deluge of logins. That means users will begin to transfer the responsibility of identification to

businesses. We'll start seeing developing technologies such as biometrics and behavior identification running invisibly in the background to verify a customer without being overt. As this trend continues, identity management will become more secure, but less visible to the consumer. There will be some friction around this in the beginning, especially with older users, as some customers will initially think the lack of gates mean their information is open to just anyone. Businesses will be tasked with providing assurances of safety to the customer while also improving background security"—Matt Ulery, Chief Product Officer, SecureAuth

"As assets become increasingly digital, and deep fake techniques improve, *cryptographic signatures will be an important tool* to push back against fraudsters an fakers"—Max Krohn, Co-Founder, Keybase

"In 2020, *we will move beyond the buzzword and see clearer definitions of what zero trust really means for enterprises and individuals*. What is currently missing is a zero-trust reference architecture—to assume everything is bad—and I foresee truer definitions coming to fruition for deploying something meaningful. With the perimeter dissolving and people working from multiple environments, zero trust will move more into the mainstream as everyone begins to buy into the vision"—Kowsik Guruswamy, CTO, Menlo Security

"As the drive toward a passwordless future continues, access will be determined by context—where you are logging in, what time, and from what device. This shift in authentication will change the need for passwords. While the methods of authenticatio will likely continue to move toward a superior biometrics-based approach, the most important authentication factor will become the context in which users are looking to gain access. Soon, opening different apps will not only rely on facial recognition or your fingerprint, but where you are, the network you're connected to, the country you're working from. *In 2020, context will be king in the world of authentication"*—Michael Covington, VP of Product, Wandera

"In the age of consumer trust, organizations need to develop a customer service strateg that is centered around consumer privacy and data security. This includes utilizing multi-channel authentication methods for customer interactions and adopting real-tim authentication (RTA) technology to track fraudsters and suspicious interactions. *In*

2020, more customer service organizations will adopt these consumer-first protection strategies with dedicated solutions for compliance, authentication and fraud prevention to address challenges related to data privacy and security"—Gil Cohen, General Manager of Multi-Channel Recording and Voice Biometrics, NICE

From what corner of the ever-expanding cyber threat landscape will attack come from? What will be the new targets and attack types? Expect lots of cyber criminal creativity plus more of the same, lots more of the same

"We expect to see a major increase in more sophisticated and resistant sextortion attacks. The *'Save Yourself'* malware is a new form of sextortion designed to both extor victims by capturing embarrassing videos and photos of them, and potentially compromise bitcoin wallets and mine other cryptocurrencies. *Sextortion attacks have become widespread and will be able to reach over 100,000 users by 2020*"—Andrew Newman, CTO, Reason Cybersecurity

"Business Email Compromise (BEC) or impersonation-based attacks will be a big them in 2020. The social-engineering aspects of such attacks are becoming more and more sophisticated and difficult to detect, and can easily be leveraged within email as well as other collaboration channels. Most importantly, *they can't be prevented by endpoint security*—only email or messaging security solutions combined with user education wil fight such attacks"—Yoram Salinger, CEO, Perception Point

"REAL ID will cause real chaos: *As the October 2020 deadline looms, REAL ID will catch several states off guard*. Expect states to scramble to meet demand for new licenses. In the rush, security will be placed on the backburner. At least one state will b caught with exposed, sensitive data on drivers. And infrequent travelers who failed to update to the new licenses will be disappointed when they are turned away at airport security and must cancel their vacation to Disney"—Brian Vecci, Field CTO, Varonis

"I envision *ransomware effectively targeting devices in homes in the next 5-10 years*. Interactive speakers, IP cameras, and other internet-connected devices like thermostat and appliances, bring more convenience and comfort into consumers' lives. We have already seen them also bring greater risks by giving cybercriminals new opportunities t access our information, and even launch attacks. Cybercriminals will focus on exploitin

consumers through these devices as we see an increase in the volume of things going into homes with a lack of built-in security controls"—Gary Davis, Chief Consumer Security Evangelist, McAfee

"It is only a matter of time before we see *a catastrophic breach of private information coming from Alexa, Google Assistant or Siri*. This would have devastating consequences, as these devices, that live in your home, listen and collect highly sensitiv personal information"—Otavio Freire, Co-Founder, President and CTO, SafeGuard Cyber

"Hackers will increasingly automate their operations to the point that *companies that not remediate security vulnerabilities as soon as they become known will almost certainly be breached*. Unpatched vulnerabilities in open source libraries will become the biggest source for such attacks"—Rami Sass, Co-Founder and CEO, WhiteSource

"The proliferation of artificial intelligence (AI) solutions for communication (e.g., Gma auto-complete*) will continue to lower the bar for exceptionally effective phishing ema at scale*. Today, it takes time to build something contextually meaningful and accurate for hopeful phishing victims, but attackers continue to leverage more and more tools and data sources (e.g., information lost to breaches) to make every phishing attack a spearphish"—David Pearson, Principal Threat Researcher, Awake Security

"Given that attacks on the web server are generally more challenging*, attackers will instead look to leverage holes and weaknesses in the browser*. The same robust development practices that are often in place for traditional apps aren't applied within the web-app world. What's even more dangerous though, is the use of thousands of third-party code libraries and JavaScript tags that are used by websites. This alone makes them especially vulnerable to a wide variety of exploits. I anticipate that these types of attacks will increase in 2020"—Jon Wallace, Security Technologist, Instart

"In 2020*, business email compromise will continue to rise* because of a confluence of three events: 1) More password dumps are hitting the market, resulting in more email/password combinations (or crackable hashes) being available to bad actors. 2) Credential-stuffing techniques have gotten more prolific and sophisticated because attackers have realized that password re-use (with small variations) is still the

predominant user practice, as password-generators and password managers haven't ye taken off in the market. 3) The primary targets of cred-stuffing campaigns are the majo cloud email providers like Gmail, O365 and Yahoo, especially on older accounts with POP/IMAP enabled, because those services do not correctly rate-limit or lock accounts with too many failed password attempts"—Kevin O'Brien, CEO, GreatHorn

"Relentless reporting of new, high-profile insider threat breaches will push many more businesses to finally take insider threat seriously enough to formalize programs and allocate more budget to protecting their IP. In 2019, at least half of data breaches involved an insider, but in 2020, this figure could exceed 60%. Companies will begin tc lean into new technologies designed distinctly for protecting from insider threat, rathe than shoe-horning in outdated technologies that are ineffective because they were neve intended for that purpose. *More than 20% of organizations will begin actively measuring what departing employees take from their organization*"—Joe Payne, President and CEO, Code42

"Insider threats, both malicious and accidental, account for a growing number of data breaches. From data theft to inadvertent information sharing, *the most significant risk often lurks in the cubicle next door*. Companies aren't powerless to address these problems, and with threats coming from all directions, it's critical that they take action in 2020"—Isaac Kohen, VP of R&D, Teramind

"Hackers are beginning to focus on more targeted attacks that will generate more revenue and cybersecurity will be a critical issue for all businesses, no matter the size. However, some businesses have still not taken a proactive approach to mitigate risks. I 2020, businesses will start to allocate more budget towards keeping their companies secure *as IT pros will see legacy tactics begin to become obsolete, being forced to update their disconnected point tools, manual processes, and lack of staff*"—Tiffany Bloomer, President, Aventis Systems

"Cyberattacks will continue to grow in breadth, scale, imagination and complexity. Sometimes they are perpetrated by 'hacktivists' that disagree with an organization's corporate stance on an issue or its wider ethical position. Sometimes attacks are state-sponsored—designed to wreak havoc and chaos and destabilize entire governments. However, the majority are still carried out by computer geeks trying to outsmart the

latest cyber protection technology or opportunists looking to make a quick buck"—Trevor Bidle, Information Security and Compliance Officer, US Signal

"Despite all the attention, money, tooling, startups and emphasis, security practitioners will still be playing a game of whack-a-mole through at least 2025. Over time automation will begin to moderate this tension but it will take at least a half a decade to begin to take hold for the vast majority of companies"—David Vellante, Co-Founder & CEO, SiliconANGLE Media

"In 2020, CISOs will start to question the strategic validity of the rapidly escalating arms race with hackers. Sure, there are plenty of effective technologies and tactics for keeping the bad guys out of your company's databases, but those solutions will always have relatively short shelf lives, as hackers today are getting better and better at finding workarounds. The hunt for optimized synergy between tech solutions and the human element will define the cybersecurity industry this year"—Mika Aalto, Co-Founder and CEO, Hoxhunt

"Over the last few years, there has been a dramatic increase in cyber-fraud, with business email compromise attacks alone costing organizations worldwide $26 billion between June 2016 and July 2019. Unfortunately, *cyber-fraud will only continue to grow in 2020,* with the volume and sophistication of attacks rising daily. Given that cyber-fraud is an extremely costly reality for modern business, more and more companies will reassess their accounting and payment controls to mitigate this incessant threat"—Alon Cohen, Founder, Chairman and CEO, nsKnox

"The reality of operating an online business is more complex than ever and is only getting more complicated. The growing usage of 3rd party vendors on eCommerce sites enables businesses to optimize customer engagement and grow revenues, but adding these digital vendors introduces new risks for protecting user privacy, regulation compliance, and other security issues. This is even more complicated due to the fact that these online retailers often lack total visibility and control into which 3rd or 4th party vendors are operating on their website and what kind of customer data they're collecting. *These blind spots are the cause of many high-profile data breaches, which will continue to plague us in 2020*"—Chemi Katz, Co-Founder and CEO, Namogoo

What specific segments and sectors of the economy will be prime targets in 2020?

"In 2020, cyberattacks will become more and more focused on having a physical impac on industry. So, for example, companies and organizations in the transportation sector with its growing focus on autonomous, connected vehicles—will view cybersecurity as a key enabler towards modernization. Subsequently, *we will continue to see more cybersecurity solutions tailored towards specific industries* and their unique technologies and business logic, and which are particularly effective for such targeted attacks"—Amir Levintal, Co-Founder and CEO, Cylus

"Banks are taking immense measures to match services offered by their digital-native counterparts, but digital transformation to attract customers isn't the only innovation area worth focusing on. There have been more data breaches this year than can be counted, shining a light on banking innovations' major blind spot: *Strategies to amass more and more data are proving not only unsafe, but redundant*. Banks should instea invest in their technical agility to react to the wide array of risk onboarded by a growing digital strategy, as well as devote resources to payment fraud prevention techniques an technologies"—Igal Rotem, CEO, Credorax

"2019 saw a record number of hospital and medical networks breached, compromising more health records and patient data than ever before. With thousands of connected medical device endpoints in every hospital and sub-par cybersecurity measures, continued ransomware and phishing will plague the industry as clever hackers eye lucrative pay days from stolen patient data. *2020 will see many hospitals continue to struggle to protect their organizations* as they begin the attempt to bridge the gap and improve lacking cybersecurity protocols"—Dustin Anders, VP of Field Engineering, CyberMDX

"As semi-autonomous truck platooning programs roll out at an increasing rate, the global trucking market is set to profit from a decrease in operating and logistics costs in addition to a decline in cargo loss issues; however, *the industry can also expect to see a uptick in targeted trucking ransomware attacks due to the added vulnerabilities that higher levels of connectivity bring, if no solution is employed*. This is why cybersecurit needs to be built from the ground up and deeply ingrained in not only the production

process of trucks, but also the design phases as well as mastered for retrofitting in the aftermarket for existing vehicles on the road"—Moshe Shlisel, CEO, GuardKnox

"*Since we can no longer rely on the traditional guns, guards and gates approach to security, we will see in 2020 greater reliance on a variety of groundbreaking security technologies* such as shot detection and millimeter wave weapon detection. These are the most advanced solutions that are powered by machine learning and computer visio a space that has only just begun to accelerate its application to securing venues and a variety of other public spaces. We see it growing tenfold in 2020"—Jeffrey Muller, Advisory Board Member, VSBLTY

What's to be done about improving cyber defense? The bigger picture... of collaboration, culture, and customer-centricity

"To be more effective in protecting themselves, enterprises have to share information about suspects and threats, but there are major barriers to such sharing: Data privacy regulations, confidentiality and even concerns about revealing the fact that an enterpri was a target of a cyber-attack. Using Privacy-Enhanced Technologies such as homomorphic encryption, it's now possible to share insights on sensitive data or to confidentially query sensitive repositories without exposing personal information or other sensitive data. *It takes a network to defeat a network*"—Rina Shainski, Co-founder and Chairwoman, Duality Technologies

"In 2020, *we will see the emergence of the 'cyber savvy' board*. Accountability for cybe and risk incidents moves up the organizational hierarchy and becomes a central issue f the CISO, C-Suite and Board of Directors. In 2020, expect mindful organizations to begin hiring board members that bring experience in risk management and informatio security as a way to prepare the business for a digital future. Gradually, this will becom a 'new normal' for the enterprise as investors pressure leadership for clear strategies or how they are managing digital risk"—Rohit Ghai, President, RSA

"In 2020, several publicly traded, Fortune 1000 companies, will face the same fate as Equifax. Due to holes in their security posture and in their third-party business partner (and lack of visibility into these issues), data breaches will plague these organizations. Corporate reputations will be jeopardized, and execs and boards alike will face severe

legal and financial ramifications. Additionally, the same lack of continuous monitoring for potential security issues will lead to data breaches that threaten major M&A activity In turn, fed up with the breaches, attacks, and frauds impacting revenue, *shareholder suits targeting board members will gain traction, forcing boards to take a larger, more informed role in cyber*. As the role of cybersecurity becomes ever more importan investors will keep a closer eye on how companies perform in this area, going so far as t incorporate cyber into their ESG analysis"—Jake Olcott, Vice President, Communications & Government Affairs, BitSight

"Security finally becomes a CX Priority: It's time for customer experience (CX) leaders *stop looking at security as just an IT issue and make it a critical part of the overall customer experience purview in 2020*. The consequences of data breaches directly impact customer loyalty, and given what's at stake, CX leaders will need to be invested finding a solution to curtail the fallout and salvage customer confidence and trust. Taking a customer-centric approach to security will require a delicate balance between providing access to information and systems that enable agents to provide a great customer experience while still safeguarding customer data"—Ryan Lester, Senior Director, Customer Engagement Technologies, LogMeIn

"In 2020, organizations, their employees, and their contractors will need to take greate responsibility when it comes to building a cybersecurity-first culture to prevent devastating breaches. *An empowered workforce is an organization's greatest data breach deterrent*. Organizations will also continue to invest in new applications and infrastructure, meaning security will need to be baked into everything from DevOps to cloud adoption, rather than relying on the SOC or endpoint security solution to secure systems after the fact"—Jon Check, senior director of cyber protection, Raytheon

"*A new wave of corporations will explicitly weave data and technology ethics into the corporate governance*. Bolstered by the Business Roundtable's letter calling for expanded stakeholder capitalism and the rise of 'B Corps,' data ethics will become standard fare of the mission-driven companies of the future"—Dan Wu, Privacy Counci and Legal Engineer, Immuta

"The chief information security officer (CISO) is among the most coveted leadership positions in the security industry, and as with other roles in the space, we'll continue to

see the role evolve in 2020. *More enlightened teams are not approaching security as just a preventative business function—they assume its broader role in business succes* With an increasingly critical role in meeting diverse needs across an organization, CISC will benefit from an established foundation that broadens the value and impact of cybersecurity"—Steve Moore, chief security strategist, Exabeam

What's to be done about improving cyber defense? The devil is in the details… of software testing, DevOps, apps, APIs, the IT organization

"*While everyone is talking about the need for security testing to shift left, security knowledge is still stuck in the right*. As a result, even when developers decide to own security testing, they choose their security testing tools for all the wrong reasons and er up using stuff that provides marginal security. Code will continue to ship with lots of vulnerabilities, exposing companies to risks and they will ultimately face breaches. In 2020, we will see traditional security testing vendors moving in and offering more developer-oriented security testing tools, and, in response to breaches, these tools will be adopted by more security savvy developers"—Shahar Sperling, Chief Architect, HCL AppScan

"DevOps capabilities will continue to increase their significance in moving projects to products, as more organizations fully embrace DevOps each year. This will drive *an increased awareness of security risks and put an additional focus on DevSecOps and how open source software is managed within projects*"—Carolyn Crandall. Chief Deception and Chief Marketing Officer, Attivo Networks

"*API security will be a priority for businesses*. Attacks on application programming interfaces (APIs) will increase in 2020, and business spend to secure them will spike as result. Unsecure APIs can lead to exposure of massive information loads, from airline ticketing to online ordering. Expect to see an increase in business spend to secure APIs in the coming year to prevent these damaging attacks"—Jonathan DiVincenzo, VP of Product, Signal Sciences

"More organizations are reaching maturity with their DevOps initiatives and modernization of the software development lifecycle. While this includes embracing strategies like microservices, companies will also see the release velocity increase for

larger, monolithic applications. This new reality will create real security challenges and risks. That's because existing security testing tools can't scale to meet the speed requirements of larger applications in DevOps environments. In 2020*, organizations will be challenged to adopt security solutions that can scan large applications*, as well as deliver critical vulnerability information how and when it's needed to make the right development decisions, without slowing down the pipeline"—Manish Gupta, CEO, ShiftLeft

"While many DevOps teams are already doing basic appsec in the CI/CD pipeline (mainly vulnerability scans), we are starting to see *a next-generation of DevSecOps which includes behavioral profiling, automatic policy generation and compliance testing for infrastructure as code*"—Reuven Harrison, CTO, Tufin

"It's impossible and unnecessary to protect everything in an enterprise at the same leve *so the next expansion that we will see in 2020 will be in the discovery, classification, and tagging of critical data* to help enterprises protect their most sensitive classified information—something that can only be handled with AI for large enterprises"—Myke Lyons, CISO, Collibra

"*As the cyber equality gap widens, calculating ROI will guide the way*. 2020 will see the cyber-economic disparity between the Fortune 100 and all other organizations wid further, meaning less-fortunate organizations will be forced to double-down on efforts leading well-positioned business returns (ROI) or quantitative risk management effort (through the use of a quantification model like FAIR)"—Jeff Welgan, Executive Directo Head of Executive & Professional Training Programs, CyberVista

"Structured and unstructured data security will be handled increasingly as one. Management of outsider threats will merge with insider threats. External and internal data will be treated as one. And data security and governance functions will also converge. *This convergence has already started and will accelerate this year, especial with new regulations such as privacy-driven GDPR and CCPA requiring a holistic vie of data security and management*"—Kon Leong, Co-Founder and CEO, ZL Technologi

It's the people, stupid—no question about it? talent, skills shortage, the future of work, automation

"Automation will become critical for businesses to secure websites, connected devices, applications, and digital identities necessary to prevent crippling and costly attacks. Ransomware attacks, data breaches, and email impersonation continue to increase as cybercriminals become more sophisticated, making it imperative to eliminate the potential for human error in cybersecurity operations. *Functions that require human intervention and are laborious and error-prone will be replaced by technologies* that automate protection of security elements at scale and prove their essential value in helping enterprises ensure compliance and establish safe internet practices"—Bill Holt CEO, Sectigo

"Despite all of the advances made in security over the past decade, it still takes organizations 15 times longer to close critical vulnerabilities than it does for attackers t weaponize and exploit them. In 2020, we'll continue to see major enterprise-threatenir breaches caused by known vulnerabilities for which a remediation was available. Organizations will have no choice but to radically accelerate the speed at which they harden their endpoints, with the most resilient adopting a new best-in-class response threshold of 24 hours for zero-day vulnerabilities and 72 hours for other critical exposures. *Automation that delivers machine speed for endpoint hardening is required if organizations are to achieve defensible outcomes*. Thus the 24/72 threshol will be the security metric that separates resilient organizations from those that suffer catastrophic breaches"—Richard Melick, Senior Technology Product Manager, Automc

"The issue of diversity still plagues the technology industry and is ever present in cybersecurity. Embracing a diverse workforce will become mandatory in 2020, and beyond, in order to meet the demands of a growing industry that's becoming more and more complicated. To offset the talent deficit, innovators will grow their cybersecurity talent through investing heavily in upskilling their current teams and bringing on junio talent. Organizations will continue to reach out into the community to mentor youth ar spread the passion for technology and cybersecurity so the next generation is prepared for cyberwars"—Stephanie Benoit-Kurtz, Director of Cybersecurity, Station Casinos, La Vegas

"Over the next year, as an industry, we will do more to close the security skills gap by broadening our recruiting efforts to uncover candidates from varied backgrounds instead of looking for 'unicorn' candidates that don't exist. *We'll see a shift in the way*

we look at resumes by placing less importance on pedigree and certifications, and we see a switch-up in interviewing processes, so that candidates are evaluated based on tru security mindset and problem-solving skills versus their ability to manage security tools"—Fredrick "Flee" Lee, CISO, Gusto

"2020 will be a challenging year for the business community and governments alike as cybersecurity attacks become more prevalent. With a critical shortage in cyber talent (roughly 3.5 million unfilled cyber jobs in the next two years, according to Cybersecurit Ventures), *it's important for large organizations to invest in individuals that can design and implement defensive technologies*. Similar to the problem the U.S. faced in World War II, we have to train millions of people quickly and then deploy them as trained professionals as soon as possible. This time, however, the domain of warfare is cyberspace"—Mark Davis, Managing Director, Fullstack Academy Cyber Bootcamp

The business of cybersecurity: The good, the bad, and the ugly

"In 2020, hackers will have security vendors in their crosshairs. *It's essential that security companies be the platinum standard for security*; if your organization has a database of exposed passwords, for example, it's critical that these be properly encrypted, hashed and stored. Boasting that this information is in plain text is like inviting a cybercriminal to your housewarming"—Mike Wilson, CTO, Enzoic

"Cybercriminals will continue to heavily invest in their businesses as new monetizatio channels emerge. During the past 3 years, the underground economy has experienced shift in how cybercriminals are monetizing their end products, from concentrating efforts on manual transactions and listings in markets, to focusing on sales of credentials, network access and sophisticated fraud methods. Instead of selling service or data listings on an individual basis, threat actors are placing more effort into buildin lasting, business-like enterprises by investing more in branding, customer support and intuitive user interfaces. Drawing inspiration from legitimate online businesses, cybercriminals use automation to help move their stock off the virtual shelves and collect data to better monetize their deliverables, further expanding the cyber threat landscape"—Raveed Laeb, Product Manager, KELA

"*The security industry will start to be held accountable by its customers and by the government*. In 2020, there will be some sort of congressional hearing where the CEOs of security companies will have to explain why their solutions didn't work and the FTC will look into enforcement action for false advertising for at least one major security vendor"—Malcolm Harkins, Chief Security and Trust Officer, Cymatic

"As the overarching security landscape continues to grow and incorporate more aspects like cybersecurity, the idea of "security as a service" will become commonplace. In 2020 we will continue to see niche companies push what they're good at, but others may *develop specific specializations and unique innovations in managed services to drive more value*"—Brad Konkle, Director of Integrated Solutions, STANLEY Security

"Enterprise CISOs and their teams are drowning in monitoring and alert workloads, struggling to hire quality talent, and managing increasingly complex hybrid cloud environments. In response, *during 2020 we should see an acceleration in the number of SaaS security vendors offering services alongside their software*. If you're selling a point solution, be prepared to explain how your customer can make use of it without taking on a lot of extra work"—Ariel Tseitlin, Partner, Scale Venture Partners

"*I believe that 2020 will be a watershed year when it comes to demand for higher cybersecurity standards in business software*. It feels like hardly a week went by in 2019 where there wasn't some kind of major cloud service breach in the news. I predict that in order to maintain trust and market positioning, more business SaaS companies are going to emphasize improved security and privacy"—Markus Mikola, Founder and CEO, ContractZen

Follow me on Twitter or LinkedIn. Check out my website.

Gil Press

I'm Managing Partner at gPress, a marketing, publishing, research and education consultancy. Previously, I held senior marketing and research management positions at NOR... **Read More**