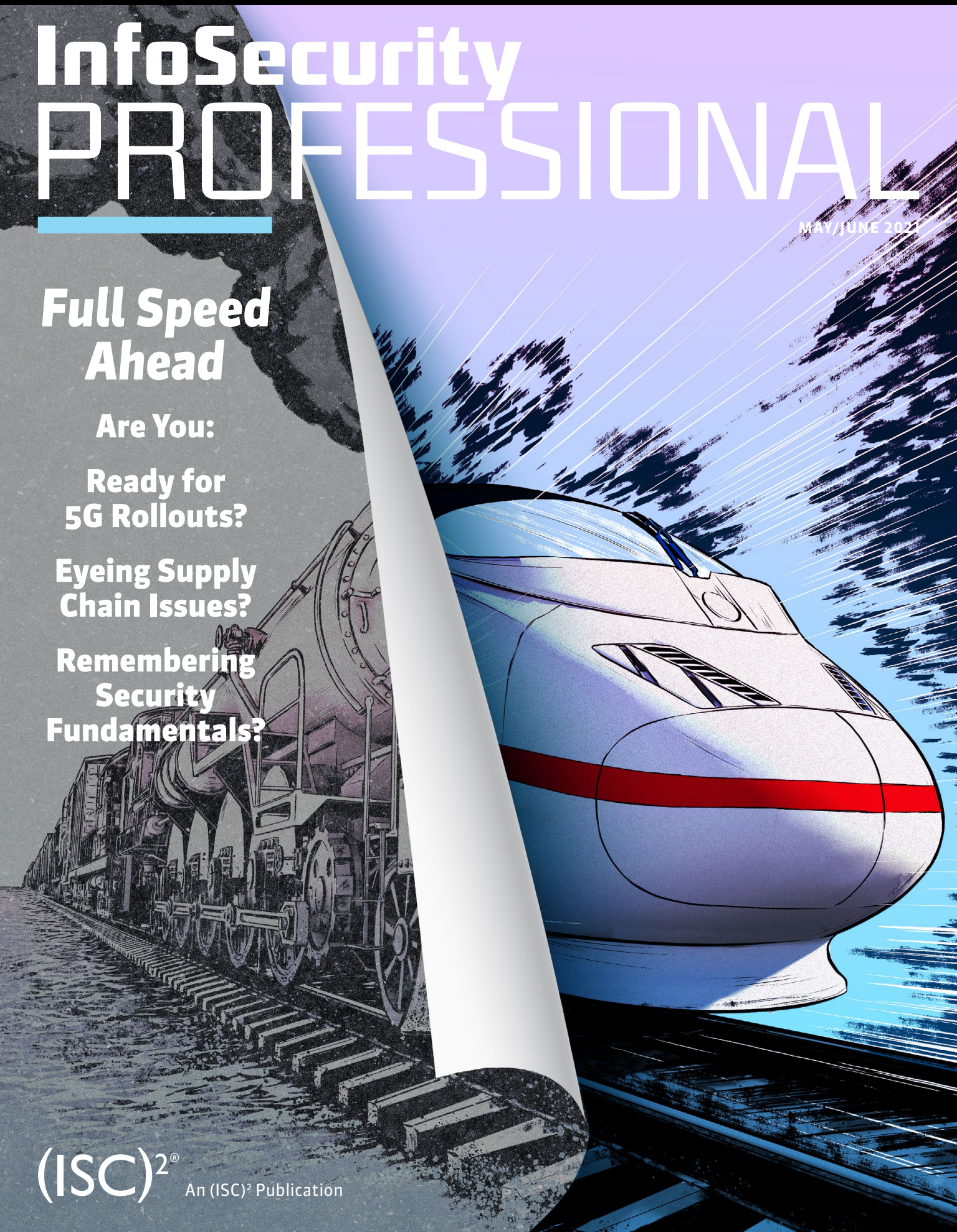
TIPS TO AVOID HIRING THE WRONG PEOPLE

InfoSecurity PROFESSIONAL

MAY/JUNE 2021



Full Speed Ahead

Are You:

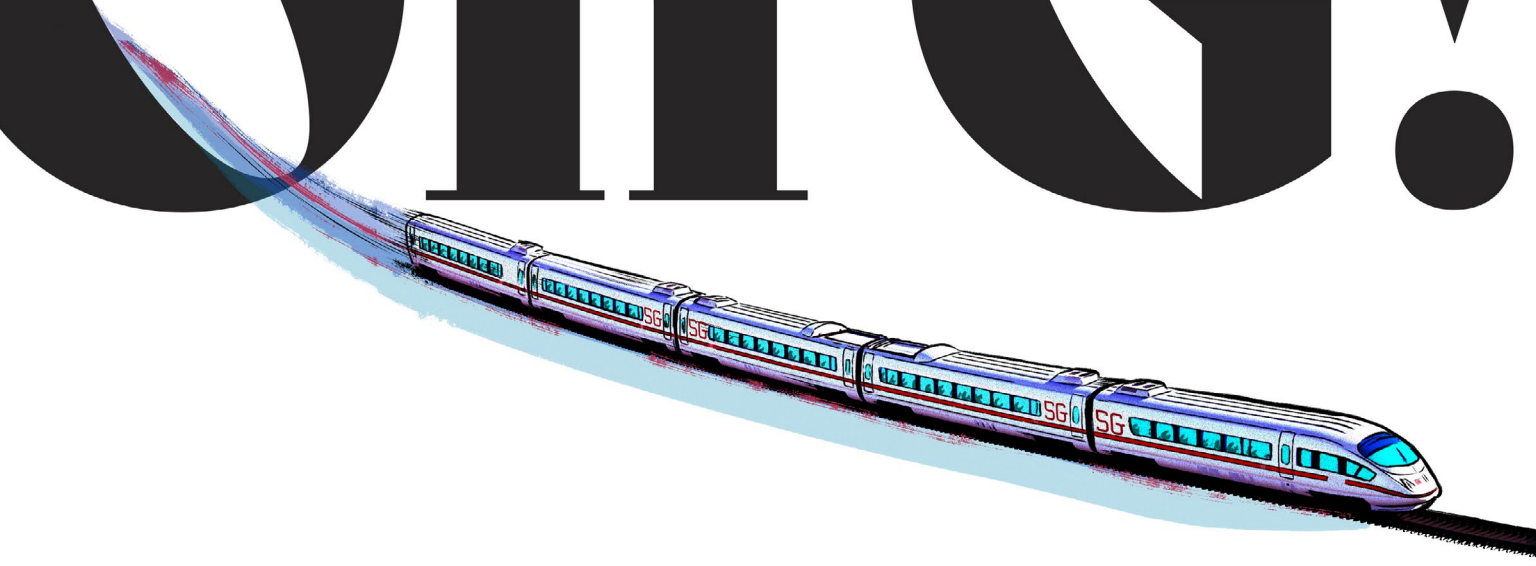
Ready for 5G Rollouts?

Eyeing Supply Chain Issues?

Remembering Security Fundamentals?

(ISC)² An (ISC)² Publication

Oh G!



Maintaining 5G security as rollouts speed along

BY ANNE SAITA

AMONG THE MANY conspiracy theories circulating at the onset of the COVID-19 pandemic was one begun by a Belgian physician who told his local newspaper that 5G *could be* biologically linked to the novel coronavirus. Soon celebrities with large online followings warned that COVID-19 might spread through 5G technology, which also was said to suppress immune systems to render people more vulnerable to the virus. Arsonists across the United Kingdom and Europe took note and torched 20 cell towers—including one that served a field hospital treating COVID-19 patients.

5G's purported COVID-related "health risks" have since been widely debunked by the medical establishment. There are, however, other threats associated with 5G that are firmly rooted in reality.

The technology's fast speeds and low latency are expected to usher in a new era of artificial intelligence-driven innovation, with the intellectual property and proprietary processes behind breakthroughs in need of strong protections. These next-generation wireless networks also will hypercharge the Internet of Things (IoT), connecting masses of more visible devices and expanding attack vectors. Additionally, the same high-throughput broadband that delivers greater flexibility and scalability for legitimate users will do the same for those with malicious motives.

ILLUSTRATION BY RAUL ALLEN

"The net benefit is going to be fantastic," says Rear Adm. (ret) David Simpson, USN, who is now a professor at Virginia Tech's Pamplin College of Business's Leadership and Cybersecurity program. "The challenges aren't meant to be showstoppers; they are meant to describe things we need to figure out."

Among those "things" are:

- A greatly expanded attack surface, given 5G elements—networks, devices, IoT sensors, actuators and terrestrial antennas, etc.—will be everywhere 5G service is available. This also will expand the IPv6 address space and make such devices more visible.
- New machine-oriented communications that will require real-time detection systems and immediate mitigations.
- Greater use of multi-access edge computing (MEC) that brings communications, computation and storage to the edge of the network, rather than these capabilities remaining within the core.
- Super accurate location access services that provide exceptional functionality but also raise privacy and security concerns as more devices and users are tracked within a 5G ecosystem.
- A need for greater coordination between service providers and customers, so everyone understands their security responsibilities within this new environment.

"The challenges aren't meant to be showstoppers; they are meant to describe things we need to figure out."

—Rear Adm. (ret) David Simpson, USN, professor, Virginia Tech's Pamplin College of Business's Leadership and Cybersecurity program

FROM ONE GENERATION TO THE NEXT

Each generation of wireless networks brings a new set of functionalities that also alters application availability and backward compatibility. This allows communications to continue with legacy infrastructure. 4G introduced capacity-building LTE (long-term evolution), a standard for wireless communications between mobile devices and data terminals that will continue into 5G.

It's the increased machine-to-machine usage that is the biggest differentiator between 5G and its predecessor. Yes, you'll be able to better stream video and group text with less drag, but the biggest benefit will be in helping convert cities, factories, medical centers, etc. into "smart" buildings designed for a much broader IoT ecosystem. This new-and-improved wireless backbone also means organizations can develop larger, more diverse data sets that become the fuel for artificial intelligence, machine learning and deep learning that until now soaked up an enormous amount of computing resources.

In addition, with 5G, the industry will migrate from hardware-oriented radio access to software-defined networks (SDN) to fully implement network virtualization once done with appliances. This also alters the threat landscape since attackers can not only compromise a wire-connected piece of hardware but also will focus on a control plane defined by code.

"We really need to be thinking about how we protect the integrity of numerous software code bases and their interconnections and assertions of integrity across a network that sees this convergence between communications, computing and storage," Simpson says.

Most are now familiar with the SolarWinds attack that threatens national security. Bad actors injected code into software that tens of thousands of organizations used to measure packet flows and monitor other pertinent network data. *(See "3 Ways to Test a Software Provider's Trustworthiness," p. 31.)*

Simpson points to a history of similar attacks where Russians have attempted to get inside sensitive networks by attacking the supply chain. In 1976, the KGB inserted eavesdropping equipment and burst transmitters in 16 IBM Selectric typewriters destined for use in the American Embassy in Moscow. Ten years ago, when he was still at the Pentagon, Russia was caught attempting to insert malicious code in the development supply chain of Netcracker Operations Support Software (OSS) used by the largest commercial and government global

networks. This would have allowed cyber attackers to infiltrate organizations by adding new code into the network security development process.

In these incidents and others like them, covert operations are presumed to originate with nation-states. "Supply chain attacks have always been a goal of our adversaries, and always will be," he indicates.

Simpson further warns: "Our high-end adversaries will seek in the very beginning to get into the elements that make up the control plane and the application content connections in the networking of 5G and the 5G user." *(See "5 Ways 5G Networks Are More Vulnerable to Attacks," below.)*

THE RISE (AND CHALLENGE) OF MEC

5G significantly alters the IT architecture within organizations and requires a new level of automation in order to protect endpoints, radio transport and radio access networks, network cores and all of the cloud-based applications moving to the edge. All will need to be carefully monitored and incidents responded to in near-real time.

"Multi-access edge computing is a big challenge because it means you're running multi-vendor data centers, cloud-based throughout your network in all sorts of different locations, so you have to consider the management, the monitoring, and incident response is critical," said Kevin McNamee, who runs the Nokia Threat Intelligence Lab, during a presentation at last November's (ISC)² Security Congress.

In essence, a lot of mobile activity done within the core of wireless networks will move to the edge, requiring cybersecurity professionals to manage the security of "mobile edge clouds," as McNamee refers to MEC, with a more distributed environment that will make it more difficult to secure. Access control will be key.

"All those servers that come in from different vendors—they're running different applications, they're running in a cloud environment, they have to be managed, . . ." he said. "From a security perspective, when you fire up an application, you want to fire up the security rules policy to support that application. All has to be done."

The threat intelligence expert told the Security Congress audience that device security is critical, to both maintain control of this new environment and to reduce the chances of the proliferation of these WiFi-connected machines being commandeered to launch massive DDoS attacks or serve as a vector for malicious code.

This is where the concept of slicing comes in.

5 WAYS

5G NETWORKS ARE MORE VULNERABLE TO ATTACKS

5G warrants a new approach to security, especially when mission- and business-critical operations are at stake. A September 2019 Brookings article co-authored by Virginia Tech professor David Simpson and Brookings Visiting Fellow Tom Wheeler outlined five ways fifth-generation wireless networks are more vulnerable than previous versions.

1. The switch from centralized, hardware-based switching to distributed, software-defined digital routing.
2. The move from hardware appliances to virtualization for many network functions.
3. Growing use of artificial intelligence within 5G networks and applications that puts machine-learning mechanisms like algorithms in a more precarious position.
4. A proliferation of short-range, small-cell antennae will become hard targets, as will the dynamic spectrum sharing capabilities they provide.
5. A much broader IoT universe full of unprotected devices. With machine-to-machine communications expanding across all industry sectors, expect more attempts to compromise cellular connectivity to interrupt transmissions and harvest data.

A SLICE OF 5G LIFE

With 5G, a telecom carrier is able to let customers break their networks into segments and protect them from each other, allowing access to different slices only as needed. This is a major security benefit, providing network separations based on the security profiles of different applications—such as those tied to medical, banking or industrial control systems.

There is a network component called the Network Slice Selection Function that defines how a device joins the network based on its identity and carrier-stored profile. A device can be given multiple slices, such as one for internet access and another for accessing a corporate network. This standard defines how a device requests and is given a slice; how the network works within that slice; and how it protects it from other traffic on other slices.

This allows security teams to apply more security controls where needed, within both the core and MEC, without impeding business functions.

Incorporating slicing to establish security zones requires careful consideration of:

- Application categories based on quality of service, throughput rates, service-level agreements and other criteria.
- Carrier-supported, end-to-end secure services that encrypt and isolate chosen segments for clients/customers.

"Who will be responsible for the security of these applications—the application vendor or the service provider?"

—Kevin McNamee, Nokia Threat Intelligence Lab

"It's very easy to say 'Secure the mobile edge cloud,'" McNamee says in a follow-up to his talk. "But I think this is going to be a big task that's going to involve a lot of people thinking pretty hard about how this is done. You have to be able to manage the security of multiple mobile edge clouds out there in the field, monitor their security and respond to incidents. There's managing the different applications from different vendors that are going to be running in these clouds. Who will be responsible for the security of these applications—the application vendor or the service provider?

"And then there's the whole aspect of access control. Who is it that gets to access the applications within these clouds? Who manages what applications that individual devices can access, and what features they can't access. What should they have visibility to and what should be restricted? These are not simple problems. We have to do a lot of work in that area."

One reason to make this a priority is the other side of slicing: a more focused target for attacks. By concentrating mission-critical and highly sensitive data into specific segments, it makes those prized slices more attractive to cybercriminals.

PRIVACY MATTERS

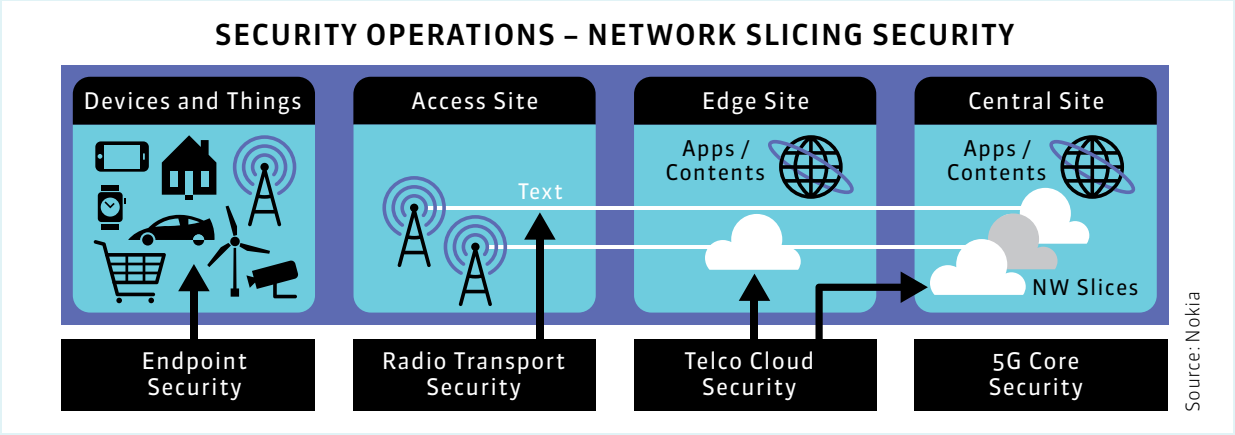
Anjali Gugle, a security architect and data governance expert who works in Cisco Systems' Customer Experience business unit, is among those concerned about privacy within 5G environments, which rely on a larger concentration of higher-frequency towers and antennae that allow hyperactive location access services. It's a great feature, she says, if you or your devices don't mind being tracked within a 5G ecosystem.

"It's going to be a ubiquitously connected kind of world; everything is going to be connected, and where I see the biggest security and privacy challenges is around sharing location and identity information—particularly personal data privacy because you'll be able to track everything, everyone, every time, everywhere," she says. "You are literally micromanaging the user. You are literally following everything like a shadow."

Those who enter "smart" buildings leveraging 5G technologies need to be aware of what happens once their device—be it a 5G-enabled smartphone, watch, tablet, laptop, etc.—accesses a network. That data needs to be protected from falling into the hands of nefarious users, especially since by then that private data is out of the consumer's control.

"The way I look at it, once you embrace and start using 5G technologies, you've given away your privacy by falling victim to hyperbolic discounting, which is a prominent decision

APPROACHING 5G SECURITY FROM MULTIPLE PERSPECTIVES



5G is designed to expand connectivity and provide a stronger platform upon which bandwidth-intensive applications, like video streaming, and technologies, such as artificial intelligence and deep learning, can be done more quickly. But this expanding ecosystem also means more protections must be in place to cover the wider array of devices, cloud services and wireless connectivity. Nokia's Kevin McNamee points to four areas that every cybersecurity professional must address.

Endpoints: Traditional 3G/4G network endpoints are primarily mobile phones that can become infected with malware. But 5G will go well beyond smartphones, laptops and tablets to any device connected to the wireless network to communicate with each other. Most of these endpoints will be built without much security by default and not be regularly updated.

Radio Transport: Expect 5G access points to continue expanding, dotting local landscapes with multiple-input, multiple-output antennae that in and of itself expands an attack surface. Then there's the radio technology utilized by 5G networks that separates a Radio Access Network (RAN) from core functions. IPsec deployments within 5G will help with authentication, but new protocols will emerge to secure radio transmissions traveling at super-fast speeds.

Cloud Services: Multi-access Edge Computing (MEC) will require a greater degree of security orchestration and automation in order to secure cloud-based, multi-vendor data centers throughout a network, of which there will be many as 5G rollouts continue.

Core Security: Running parallel to the MEC will be a new protective control plane at the 5G core. Splicing will allow for high-risk assets to be segmented and better protected when resources are limited. But it also will expand how many slices must be managed.

heuristic that can affect privacy decisions," Gugle warns. "You're giving away your data and subjecting yourself to being tracked 24/7 because you want to use their services."

Data-centric regulations like the EU General Data Protection Regulation and, in the United States, California Consumer Privacy Act will help push companies to maintain strong data governance and provide transparency in their usage of data generated by geolocation tracking.

MANAGING RISKS TO MAKE 5G WORK AS INTENDED

Risk management must be reassessed with any 5G rollout. That is, security implications will need to be balanced by the benefits a 5G environment provides. There also will be security responsibilities to be meted out between providers and those they serve.

"If somebody can magically come up with a way to protect the digital trail of a customer while providing more robust facilities, it will be a good thing."

—Anjali Gugle, security architect and data governance expert, Cisco Systems

"5G definitely is a positive thing, especially if there is accountability. It's improving location precision, ubiquitous connections and mass connectivity in a multi-vendor environment," Gugle says. "But the lack of location privacy due to the amount of tracking will remain a major concern. If somebody can magically come up with a way to protect the digital trail of a customer while providing more robust facilities, it will be a good thing."

Virginia Tech's Simpson agrees.

"You've got to bring your business objectives in a 5G world into your risk management process today. That means you start to build appropriate skill sets within your company based on how you intend to utilize 5G at your company," he advises. "You may actually reduce people in a given area because you'll rely on more automation made possible by 5G. That means it's all the more important that you bring some 5G transformation expertise into solution development transition and your objective business operation.

"Then work on risk mitigation efforts that include architectural changes for how you'll implement these capabilities," he continues. "If we just rely on acquiring a new appliance or a 5G-certified service, you'll miss many potential satisfying risk mitigations that could apply to your 5G-enabled business operations. Transformational leaders should give business risk reduction a front-row seat as they plan to achieve automation, AI and other worthwhile 5G functional goals."

ANNE SAITA is editor-in-chief of *InfoSecurity Professional*.