SECURING THE CLOUD

Experts suggest boosting efforts to keep data safe in the 'new normal'

By Suzanne Wright

THE SUMMER OF 2017 was filled with cloud activity — and not just the weather-related kind.

Week after week, anxiety mounted among IT professionals and the general public as headlines blasted news of another high-profile, cloud-centered data breach.

Whether perpetrated by individual hackers or nation-state actors, respected companies in nearly every sector, including Deloitte, Equifax, HBO, Verizon and Whole Foods, were targeted, resulting in the exposure of sensitive data belonging to millions of Americans, including credit card and Social Security numbers.

With more cloud centralization — whether private, public or hybrid — comes greater exposure, leaving cloud providers, companies and government agencies scrambling to bolster their cybersecurity defenses.

Attacks are both prevalent and expensive; think "when," not "if."

According to a June 2017 study sponsored by IBM Security and conducted by Ponemon Institute, 1 in 4 organizations will experience a data breach; the average cost per incident is $3.62 million.

Michael Bahar leads the U.S. cybersecurity and privacy practice team at the legal services firm Eversheds Sutherland in Washington, D.C., and is a former deputy legal adviser to the National Security Council and former minority staff director and general counsel for the U.S. House Intelligence Committee.

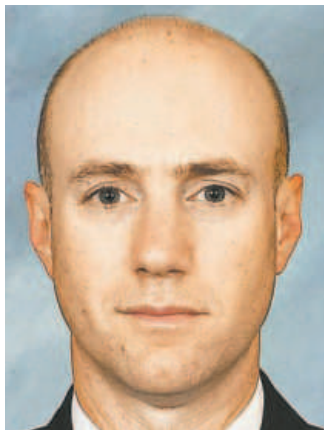
"Particularly this summer, we've (seen) attackers going further — to extortion, data manipulation, disruption and even destruction," said Bahar. "What is increasingly critical is to respond to the rapidly evolving new normal."

Bahar says cyber plans and policies crafted in 2016 to protect against ransomware may be out-of-date based on current threats such as the WannaCry ransomware attack in May that crippled more than 200,000 computers in 150 countries. Hospitals, banks, telecommunica-

CONTINUED »

ILLUSTRATION: LISA M. ZILKA

Michael Bahar
Eversheds Sutherland



DUPONT PHOTOGRAPHERS

Sara Mosley
DHS

STEVE BARRETT/DHS

Peter Tran
RSA Security

RSA SECURITY

Valecia Maclin
Raytheon

RAYTHEON

tions companies and warehouses were locked out of their data and perpetrators demanded they pay a ransom or lose everything.

"Regulators, such as the SEC, are trying to emphasize to entities a continuous culture of updating policies," he said.

CYBERSECURITY IS A BUSINESS IMPERATIVE

In response to growing threats, President Donald Trump issued an executive order in May outlining plans to bolster cybersecurity among federal agencies to safeguard critical U.S. infrastructure.

Since 2010, agencies have transitioned hundreds of locally hosted applications and data center resources to commercial cloud providers, including mission-critical applications, such as email and public-facing web services, to commercial cloud platforms.

Sara Mosley, acting chief technology officer in the Department of Homeland Security's Office of Cybersecurity and Communications, said with so many federal departments and agencies utilizing a shared cloud environment, there are challenges centering around the security, ownership and location of data, and this paradigm shift.

"While some agencies may have had a contractor-owned, contractor-operated operating model, they were in control of the requirements driving the security architecture of the data center," Mosley explained. "Cloud introduces the concept of shared tenancy and with it, the relinquishing of specialized requirements by each and every tenant."

In a cloud model, the infrastructure is owned and operated by the Cloud Service Provider (CSP). Depending on the service model of the CSP, the responsibility of the operating system and even the application could be owned by the CSP as well. While the CSP is the "operator" of the infrastructure, the security risks are still owned by the end customer — in this case, the government agency.

Mosley says the choice to use cloud technologies is largely up to the individual departments and agencies.

"The decisions are normally based on the security requirements for the data and the risk appetite for that department or agency," she said.

So how does the U.S. government safeguard data?

"The General Services Administration's (GSA) Federal Risk and Authorization Management Program (FedRAMP) has provided a baseline for the CSPs offering services to the federal government," said Mosley. "FedRAMP is a governmentwide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services."

FUTURE-PROOFING STRATEGIES

According to a 2016 report from RSA Security, a Bedford, Mass.-based computer and network security company, 90 percent of organizations are dissatisfied with their threat detection and response time.

Bahar says an attack on one organization is an attack on all. But the upside is that it catalyzes information sharing.

"Each cyberattack is the equivalent of a wakeup via a heart attack," said Bahar. "When the attack is in your industry, everyone improves security."

Experts agree that a multipronged approach is necessary.

When it comes to assessing the threat landscape, Peter Tran, general manager and senior director at RSA Security's Worldwide Advance Cyber Defense Practice, advocates a 360-degree, business-driven approach to security decisions. They can be distilled as the three Rs.

"We can retire outdated security technology and stop playing whack-a-mole with patching; realign monitoring to high-value areas of the business; and reinvest dollars to balance security visibility across people-process-technology," Tran said.

Bahar counsels companies' top leaders to instill the importance of "cyber hygiene" throughout their organization's culture, imbedding threat education into daily operations.

"It's like washing your hands frequently during cold season," he said. "These attacks are remarkably unsophisticated and deeply human. You don't need to be technically savvy to adopt good practices, like not clicking on suspicious links."

Bahar says organizations can also augment internal IT expertise with external consultants who have experience in the frequently targeted energy, financial, health care and high-tech industries.

Valecia Maclin is the director of cybersecurity and special missions for Raytheon's government customers.

"We should not fear the cloud; in many instances it provides more resiliency for data. But it's important to establish a baseline for your cyber risk. What are your assets? What is the state of your risk? What steps are you taking to move to a more resilient environment tomorrow?"

Both Bahar and Maclin stress the importance of improving the depth of cyber talent moving forward.

"When designing software, we can't just be great coders or innovators," Bahar said. "We must move from more of a craft to a discipline."

He offers an analogy. "We have a beautiful bridge, but will it withstand vehicular traffic and crosswinds?"

Maclin is encouraged by the level of information sharing between the public and private sectors to protect our economic and national stability.

"We are stronger together when we leverage our expertise," he said.

SAFEGUARDING YOUR DATA

"Tools exist to protect all organizations against cyberattack," says Manuvir Das, senior vice president and general manager for Dell EMC's unstructured storage division. His tipsheet includes four best practices that should be implemented across the enterprise.

AUTHENTICATION
"Prove to me you are who you claim to be with a username and password for first-level security prompts." Second-level safeguards include codes texted to mobile phones, Social Security numbers or date of birth.

AUTHORIZATION
How much access should an individual have to data? Can she create files, or read-only? Only those in her department? "You need to set a policy and permissions for every person across an enterprise."

AUDITING
No system is foolproof. That's why it's important to create a record of who accesses data, so it can be reviewed forensically if a breach occurs. "Think of it like security cameras in the subway."

ANOMALY DETECTION
Closely related to auditing, this is where you track patterns of typical activity. Did a staffer open a file, then start doing something else? How many files did he copy over what period of time? "If activity doesn't match, bells should start ringing."

— Suzanne Wright