Protecting Multi-Cloud Environments and Rebuilding Trust After a Breach

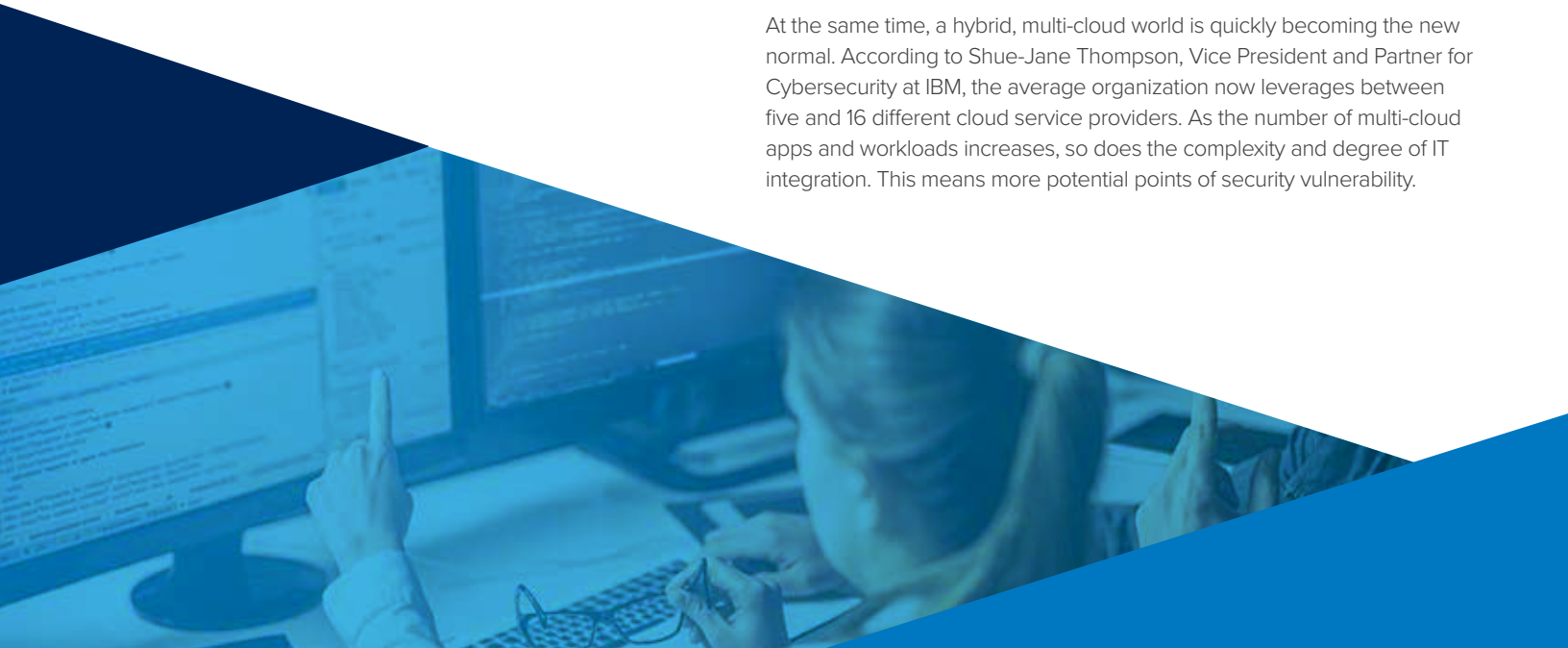
How to tackle some of government's biggest cybersecurity challenges

The average organization now uses between five and 16 different cloud service providers. As the number of multi-cloud apps and workloads grow, so does the degree of IT integration. This means more potential points of security vulnerability.

The cybersecurity threat landscape is evolving, again. In 2017, ransomware attacks like WannaCry crippled hundreds of thousands of companies in multiple countries. By 2018, ransomware threats declined and a new form of attack — cryptojacking (the theft of computing power to generate cryptocurrency) — emerged. According to the IBM X-Force Threat Intelligence Index 2019, cryptojacking grew 450 percent in 2018.

It remains to be seen which new risks will emerge in 2019, but threats never stand still as cybercriminals continually shift tactics to avoid detection. And whether it's a cybercriminal across the globe or an employee down the hall, threats to data are harder to detect and prevent today than ever before. It's no longer a matter of if an organization will be attacked, but when.

At the same time, a hybrid, multi-cloud world is quickly becoming the new normal. According to Shue-Jane Thompson, Vice President and Partner for Cybersecurity at IBM, the average organization now leverages between five and 16 different cloud service providers. As the number of multi-cloud apps and workloads increases, so does the complexity and degree of IT integration. This means more potential points of security vulnerability.



Building a Security Ecosystem

A combination of proven technology, awareness and adequate cyber workforce can help agencies limit potential cybersecurity damages and — should the worst occur — help rebuild trust with stakeholders following a breach. To secure multi-cloud environments, government leaders need to align people, processes and technology into an "ecosystem of trust." According to Thompson, sustaining that ecosystem requires a balanced strategy from three cyber maturity capabilities: cyber hygiene to ensure you've taken all steps necessary to protect your cyber ecosystem; cyber intelligence to forecast and preempt threats; and cyber resilience to enable you to continue operating during — or recover after — an attack.

Building a solid security ecosystem is not easy. Many agencies lack visibility into the activities of rogue users or cybercriminals who may have gained access to their ecosystems. They also may not know what data to collect to detect these intrusions, and their current security systems may be unable to share threat information across their enterprise. To protect themselves, agencies must gain visibility of their threat environment with threat intelligence that cuts through the noise created by false positives.

Gaining the skills and resources to implement necessary security capabilities is another challenge. Some experts predict there will be a global shortage of two million cybersecurity professionals this year. This highly competitive environment is particularly problematic for government agencies, which typically can't match private sector salaries.

These pressures are prompting more agencies to consider private sector security service providers for help. Security-as-a-Service or managed security services help agencies manage and mitigate threats while letting them maintain transparency and control and focus on their missions. These security services can provide integrated tools, service capabilities and qualified resources to jointly counter emerging threats. Proven service providers can help agencies gain better visibility into threats and operate under a cyber ecosystem to adapt as regulatory conditions change.

Because tracking and mitigating threats is their core mission, private sector security firms also can help agencies plan for

To secure multi-cloud environments, state and local government IT leaders need to align people, processes and technology into an "ecosystem of trust."

future threats. Experts say cybercriminals already are exploring how to weaponize artificial intelligence (AI) to outsmart defenses. And other burgeoning technologies like quantum computing, IoT and blockchain may provide cybercriminals new avenues into agency networks.

But good cybersecurity isn't just about technology and planning — it also includes preparation and practice.

"When it comes to cyberattacks, people tend to pull together their plans and think they are prepared," says Thompson. "But until they practice it, they don't realize there are pieces and parts that need fine tuning and rehearsal."

Rebuilding Trust

Finally, private sector technology partners can help agencies recover from cyberattacks, reduce the impact of the event and gain insights from the experience.

"It's one thing to learn from an incident, and another to successfully translate the lessons into policies and procedures," says Thompson. "Trust is probably the hardest thing to build and the quickest and easiest thing to break. A strong security program is a core part of building or rebuilding trust."

Given the constantly evolving cybersecurity landscape, the more help an agency can get, the better. According to Thompson, IBM has monitored cybersecurity vulnerabilities for more than 30 years. During that time, the company has seen some 140,000 unique vulnerabilities arise. About 41,000 of those have emerged over just the last three years.

"Cybercrime is an opportunity rich environment," says Thompson. "It takes constant vigilance, but if all parties work together, we all have a better chance at success."

This session is part of the IBM Government Cloud Virtual Summit, a free, online event featuring 17 sessions with insightful keynotes, illustrative case studies and deep dives into job-critical topics for government leaders. To view any of these sessions, visit www.govtech.com/ibmvirtualsummit