CISO Guidance: Adapting to the Cloud Era of Cybersecurity

Cybersecurity has been rapidly moving to the cloud, driving organizations to cloud-based solutions from third-party vendors instead of self-owned and maintained network security devices and software. One such cloud offering is Secure Access Service Edge (SASE) which is based on a combination of Software-Defined Wide Area Network (SD-WAN), Security Service Edge (SSE) and Zero Trust Network Access (ZTNA). This service offers scalability, flexibility, cost-efficiency, and innovation that empowers organizations to support remote work, cloud migration, and digital transformation initiatives in ways non-cloud delivered technologies cannot.

But these new technologies also bring some challenges and risks to organizations from complexity, compliance, and governance. By design, SSE and ZTNA offerings do not allow enterprises to have control over versions and upgrades that they would normally have when managing their own network security appliances (e.g., firewalls). And SSE and ZTNA offerings are likely to have different (hopefully better) security standards and practices than an enterprise's in-house cybersecurity program.

As the CISO role evolves with these moves to the cloud, CyberRatings recommends that CISOs adapt by shifting priorities from operating security programs to overseeing (monitoring and auditing) outsourced security programs.

KEY FINDINGS

- SSE and ZTNA[1] are the new standards for network security in the cloud era. They offer scalability, flexibility, cost-efficiency, and innovation. They also make it possible for organizations to support remote work, cloud migration, and digital transformation initiatives.
- SSE and ZTNA also pose some challenges and risks for CISOs. They require organizations to adopt a cloud-native approach that may not work with their existing legacy systems and processes. SSE and ZTNA may themselves also rely on third-party cloud service providers that have different security standards and practices than their own, or the organizations they are protecting.
- The CISO role is evolving as cybersecurity moves to the cloud, with emphasis shifting from operating to overseeing (monitoring and auditing).

RECOMMENDATIONS

- Communicate the need to prepare for the cloud era of cybersecurity to all appropriate executives and directors (e.g., CEO, CIO, CFO, and the Board). Clearly explain the types of organizational changes required and gain their support.
- Build a strategy and plan for the shift in priorities from operating security programs to monitoring and overseeing outsourced security programs.
- Write clear contracts with cloud service providers and vendors that define the security partnership and develop oversight programs with regular reviews and audits.
- Evaluate the skillsets of employees and change the culture of the cybersecurity program from operational excellence to outcome excellence.
- Hire specialist firms to conduct security audits, assessments, and oversight of cloud security providers.

[1] ZTNA is both a subgroup of SSE and also a distinct technology that does not require implementation of the rest of SSE

ANALYSIS

Cybersecurity has been quickly moving to the cloud. This is a significant change in which organizations use cloud-based solutions *owned and maintained by third-party vendors* instead of purchasing and maintaining their own network security devices and software. One such cloud offering is Secure Access Service Edge (SASE), based on a combination of Software-Defined Wide Area Network, Security Service Edge (SSE) and Zero Trust Network Access (ZTNA). This service offers scalability, flexibility, cost-efficiency, and innovation. SASE also makes it possible for organizations to support remote work, cloud migration, and digital transformation initiatives in ways non-cloud delivered technologies cannot.

But these new technologies also bring some challenges and risks to organizations managing complexity, compliance, and governance. SSE and ZTNA offerings (by design) do not allow enterprises to have control over versions and upgrades that they would normally have when managing their own network security appliances such as firewalls. And SSE and ZTNA offerings are likely to have different (hopefully better) security standards and practices than an enterprise's in-house cybersecurity program.

ORGANIZATIONAL CHANGES: MONITORING & AUDITING VS. OPERATING

We recommend that CISOs adapt by shifting priorities from operating security programs to overseeing (monitoring and auditing) outsourced security programs.

While operating a security program means running the cybersecurity program on a day-to-day basis, including overseeing the security devices and software, auditing outsourced security programs requires checking the quality and effectiveness of the cloud-based solutions that provide network security services for the organization. To that end, we recommend that CISOs evaluate the skillsets of their employees and the culture of the cybersecurity program as priorities shift from operating to overseeing.

Do current employees have the right skills and mindset for their new roles and responsibilities? Can the right training and development opportunities help them move from an operations day-to-day role to a monitoring and oversight role? Are they able to check the quality and effectiveness of the cloud-based solutions that provide cybersecurity services for the organization? In which cases should new employees be hired?

Often, cybersecurity practitioners avoid audits of their work, as they see them as intrusive, disruptive, or threatening. Now they will be the ones doing audits of third-party work (SSE, Managed Detection and Response (MDR), ZTNA providers, etc.). This requires a culture change that welcomes audits as a tool for oversight and an opportunity to develop best practices and adopt them within their own security programs. To make the transition as smooth as possible, CyberRatings recommends creating a clear career path and progression plan for employees, as well as clearly defined roles, responsibilities, expectations, goals, and outcomes of each position in the cybersecurity program and how they relate to the oversight function. Ideally, employees will go from avoiding oversight to welcoming oversight.

To create this culture change, CISOs may want to take some steps:

- Communicate the vision and goals of the cybersecurity program and how oversight and auditing support them.
- Encourage a mindset that welcomes feedback, seeks improvement, and values transparency and accountability.
- Foster collaboration and trust with their external partners by communicating regularly – sharing information and feedback. Resolve any conflicts promptly and constructively.

THE ROLE OF THE CISO IS EVOLVING

The cloud era of cybersecurity is approaching quickly. CyberRatings recommends that CISOs communicate the need to prepare for this change to all appropriate executives and directors (e.g., CEO, CIO, CFO, and the Board). CISOs should prioritize the time needed to develop a strategy and action plans for evolving their organization's capabilities from operating/running security programs to overseeing/monitoring security programs that are run by others. Include compliance with regulatory requirements in your planning, and the cost of monitoring and overseeing third party vendors in your ROI calculations and budgets. We also recommend CISOs develop a discrete program for identifying the roles required to execute their cloud strategy and the skill sets needed for each role. And we recommend CISOs devise a plan to migrate the culture of their company's cybersecurity program to one of operational oversight.

QUESTIONS FOR READERS

- How are you adapting to the cloud era of cybersecurity?
- Have you communicated the need to plan for these changes with all appropriate executives and directors?
- What are some of the benefits and challenges of using SSE and ZTNA models within your organization?
- Do you know what your cloud era organizational structure should look like?
- What roles will be required moving forward? What skills are required for each of those roles?
- How do you plan to evaluate the skillset of your employees?
- How do you plan to alter the culture of your cybersecurity program?

REFERENCES FOR FURTHER READING

- CyberRatings.org: Choosing the Right ZTNA Offering
  https://www.cyberratings.org/research/
- Gartner: The Future of Network Security Is in the Cloud
  https://www.gartner.com/en/documents/3981249/the-future-of-network-security-is-in-the-cloud
- Forrester: The CISO's Guide To SASE
  https://www.forrester.com/report/The+CISOs+Guide+To+SASE/-/E-RES161766#
- ISACA: Auditing Cloud Computing
  https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpaudcc
- NIST: Cybersecurity Framework
  https://www.nist.gov/cyberframework
- COBIT 2019 Framework: Introduction and Methodology
  https://www.isaca.org/resources/cobit/cobit-2019-framework-introduction-and-methodology
- Cybersecurity Audit Certificate Program
  https://www.isaca.org/credentialing/cybersecurity-audit-certificate

AUTHORS

Vikram Phatak, Thomas Skybakmoen

CONTACT INFORMATION

CyberRatings.org

2303 Ranch Road 620 South

Suite 160, #501

Austin, TX 78734

info@cyberratings.org