Shared Services Provider Concentration & Cyber Risk

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Shared Services Provider Concentration & Cyber Risk,” on May 19, 2022.

ACF members are raising important questions about concentration risk and cyber resilience. Are enterprises too reliant on a handful of providers? If a significant incident occurs, how should incident responders and cloud service providers (CSPs) prioritize support? What steps should enterprises take today to mitigate concentration risk and improve resilience? In this session Forum members shared solutions and best practices for maintaining enterprise resilience.

This roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

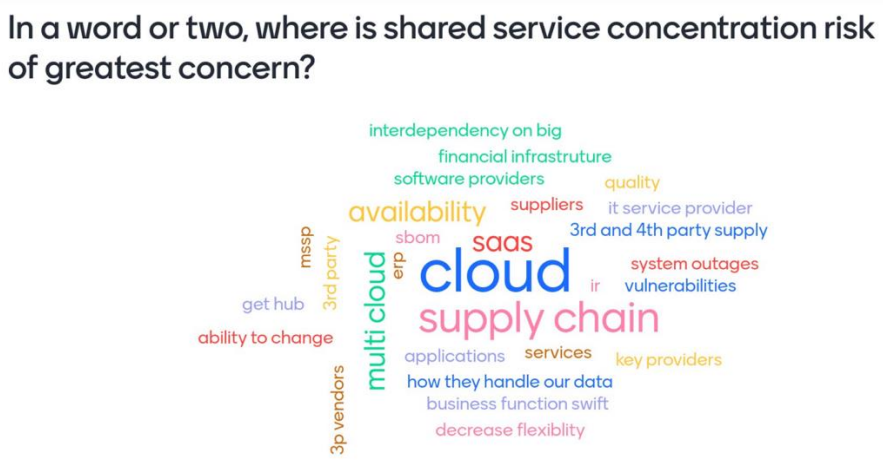
Below is a brief summary of the call:

Cloud concentration risk

A multi-cloud strategy has advantages in terms of security, operational resiliency and opportunities to leverage CSP innovations. A Forum member expressed confidence in the ability of CSPs to deliver security, adding: “They’re surrounded with smart people.” Another said, “Frankly, the cloud is more of a commodity. I think the risks are greater where we rely on more specialized assets.” “The cloud gives us options we didn’t have with on-premise computing models,” said another.

However, not every member endorsed a multi-provider cloud strategy. “Having the risk in one place where you can see it clearly isn't necessarily a bad thing," said a Forum member "The risk will always exist, but if you have to treat it multiple ways, you have a lot of cost and potential visibility issues.”

In fact, Forum members most frequently identified the cloud when asked which shared service concentration risks are of greatest concern.



A common concern: holding down costs when over-reliant on a particular CSP. “Before you make a final decision about picking a vendor, think carefully about your termination strategy,” said a subject-matter expert. Said another Forum member: “Vendor lock-in is clearly on our minds. The other side of lock-in is the opportunity lost when there are capabilities at another provider that are stronger or a better fit for a business problem.”

Other Forum members expressed concerns about single-source CSPs going off-line because they were uncertain about cost-effective alternatives.

Incident response risk

In a world of finite incident response capabilities, CISOs must have a deep understanding of service level agreements (SLAs) and contract terms and conditions (T&C) but must also be realistic about the enterprise’s ability to “consume” support, said a subject-matter expert. “Don’t assume your own incident response team is prepared to take that 3 am phone call,” he said. “Know your responder and make sure they know you,” he added. That goes beyond T&Cs. A deeper relationship can prepare both sides for a more effective incident response.

CISOs should consider that when broad attacks occur, “syndicating the solution” helps everyone. “When an incident responder helps one company with, for example, a malware attack, they should work collectively to deliver a solution that benefits the entire community,” the subject-matter expert said.

Supply chain concentration risk

Forum members expanded the discussion about concentration risk to include the broader manufacturing supply chain and second and third-level suppliers. This is an area where CISOs can contribute valuable insight but would be well-served to partner with colleagues in other departments who also have risk management responsibilities.

The idea is to think of concentration risk from the perspective of threat actors, said a subject-matter expert. They are often prepared to go “low and slow” to avoid detection while seeking vulnerabilities that extend across multiple elements of an industry supply chain. “The commonality of suppliers and software, and the risk of a concentrated attack, are what keep me up at night,” said a Forum member.

The board's concerns about concentration risk

A board member encouraged CISOs to take short- and long-term views of concentration risk. "The road to hell is paved with good intentions," he said. "We need to take a step back and analyze the problems concentration risk has created today. But because we're operating in a very broad, dynamic ecosystem, we should also be looking 10 or 15 years down the road." A Forum member pointed to changes in chip fabrication as an important lesson. "Just look at the history of the chip and wafer industry and the dominance of Taiwan Semiconductor. The US drank the Kool-Aid of the 'flat world' and now we have to be careful about outsourcing security."

Another board member said that CISOs should be able to tell a compelling story about concentration risks and how they might impact strategy. That opportunity may not come during a traditional, agenda-packed board meeting. But CISOs, along with other enterprise risk managers, should share responsibility to raise concentration risk concerns and how they are being addressed with individual board members.

Leading practices

- **Create a framework** with a clear definition of concentration risk relevant to your enterprise; metrics to measure risks over time; and specific "triggers" that could drive management to take action.
- **Consider a termination strategy upfront.** Decide how to maintain resiliency and migrate to other service providers when terms and conditions are breached, or service levels fall short. For example, several Forum members thought relationships with multiple incident response resources were appropriate. "Stay loosely coupled, and maintain the ability to shift quickly," said a subject-matter expert.
- **Test concentration risk hypotheses across multiple dimensions.** Think of worst-case scenarios and analyze how the concentration of assets and an over-reliance on suppliers contributes to enterprise risk. Exercise your responses and strengthen weaknesses, particularly relative to the crown jewels of the enterprise. Get other stakeholders involved in your scenario planning. "Concentration risk is not something we as CISOs can solve on our own," said a subject-matter expert.
- **Reinforce that concentration risk is a risk to the business.** "We're all dealing with concentration risk across different dimensions—vendors, technology, geography, industry-specific," said a Forum member. Another member added: "One concept I am pushing hard is banning the term 'cyber risk.' There is no cyber risk, only business risk."
- **During an attack, collaboration can bring solutions to the market more quickly.** "When there's a common problem, keep in mind that when we help the first one, we help everyone," said an experienced incident responder. This can be particularly important in industries where the supply chain relies on common, often interconnected assets.
- **Look deeply to uncover interdependencies.** Analyze how concentration risk in one area of the business might jeopardize other functions internally, or even the broader extended value chain.
- **Know your suppliers, and make sure they know you.** Invest time in truly understanding the security capabilities of your CSPs and other providers and develop contingency plans

that address the most important risks. Regularly review the terms and conditions in your service level agreements and be willing to pay for SLAs that guarantee service delivery. A subject-matter expert saw value in listening to cloud providers about new, value-added capabilities.

CONTACT

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.