Deloitte.

Dan Kinsella
Partner, Deloitte Advisory
Deloitte & Touche LLP
dkinsella@deloitte.com
+1 402 997 7851

Dan Kinsella is a Deloitte Advisory partner serving as the Deloitte national Third Party Risk Management leader. Dan combines business and technology solutions to help his clients create and optimize their extended enterprise. Dan is also one of the Firm leaders on our Service Delivery Transformation integrated market offering focused on our improving client's efforts in shared services and outsourcing environments.

@Deloitte

www.deloitte.com/us/servicedelivery

USServiceDelivery-Transformation@deloitte.com

How managed services can be leveraged to move the needle on cyber risk

Cybersecurity today is an omnipresent concern. As organizations ponder how to get better at being secure, vigilant, and resilient, they must also consider how to do it practically and affordably. Somehow, they must find a balanced way to respond to the asymmetric threat of cyber risk, and in many instances, managed services can help—particularly when the managed service provider has the ability to operate at the nexus of technology, risk management, and within the context of the organization's industry and regulatory environment.

Why should organizations consider managed services when transforming cybersecurity service delivery?

Outsourcing certain cybersecurity functions to a managed services provider is one of the bigger levers that an organization can pull to help improve its ability to manage cyber risk. Fundamentally, managed services can facilitate access to the right people and technologies as well as improve processes, thus shortening the timeline to better capabilities, and reducing the cost curve, as in many instances, managed services cost less than building internal cybersecurity capabilities.

The value proposition for using managed services to transform cybersecurity service delivery is attractive because cyber risk is an asymmetric threat—you can pour tremendous time, talent, and treasure into solving the problem, but one "kiddie script" hacker can take down a network if they have the right information and the will to do so. Often, outsourcing to a managed services provider can be the most effective option since it's extremely difficult to attract and retain qualified technical talent in today's competitive market. In addition, the technology required to do cybersecurity right is highly complex, it changes rapidly, and it's expensive.

In essence, the ability to become threat-intelligent is getting harder. It requires specific skills and access to data in unique places—it's not just about vulnerability management, log monitoring, and patching anymore. It's more nuanced, involves managing risk, and building situational awareness within the context of your business.

What particular cyber services should be considered for outsourcing to a managed service provider, and which should be retained?

It depends on your risk tolerance and what kind of information is used in your business. The riskier your data is, the more careful you should be about how to protect it and who is involved. For instance, does your organization have personally identifiable information, financial data, health records, etc.? What requirements are necessary to safeguard that data and to comply with the regulations regarding it? The answers to these types of questions will determine which cyber services make sense to outsource.

Right now in the market, we're seeing companies outsource some of the more straightforward, commoditized components of cybersecurity, such as penetration testing, as well as some of the most complex elements, such as security incident and event management. As the

complexity of the outsourced service increases, so should your ability to effectively manage third-party providers, both in terms of ensuring they deliver against requirements and in working with them to resolve cybersecurity concerns.

How should organizations monitor and improve the managed services received from providers?

Clear performance and risk indicators need to be identified upfront and agreed to contractually in service level agreements. In addition, someone in-house must be accountable for owning the services and the outputs. This individual or team should periodically evaluate scorecards and have an open, ongoing dialog with the managed service provider(s).

Furthermore, it is essential to select a provider that is both trusted in the marketplace and focused on tailoring services to meet your specific needs—not just providing out-of-the-box services. One of the biggest reasons for failure in managed cyber services is "the square peg/round hole" approach. Out-of-the-box managed services may be specifically tied to particular technologies which may not be a good fit. They also may not move the needle very far in terms of meeting the specific industry and regulatory requirements while also enhancing an organization's ability to manage cyber risk. These expectations require upfront selection and agreement and a provider that is the best fit across these areas in order to deliver on the promises of effectiveness and efficiency.

Ultimately the provider that can effectively enable you to manage cyber risk through the delivery of the right foundational technology and with a team that speaks your language will be the one to help deliver the greatest value.