Connectors
Cyber risk management—How can you practice cyber risk management in tandem with secure service delivery
In the realm of global business services, outsourcing, and shared services, cyber risk is quickly rising in importance, largely because companies are making big changes in those areas—in some cases fundamentally rewiring the ways in which processes and technologies are coordinated to deliver services. That’s a recipe for opportunity—and for cyber risk.

When an organization transforms its approach to any part of its business, one of the primary questions is often “what are the tax implications?” It’s a necessary question that switched-on leaders ask. In the same way, such shifts are triggering forward-thinking leaders to ask the necessary cyber security question: “How is our organization exposed further to cyber risk as a result of these changes?” It’s a particularly relevant question in the arena of service delivery transformation, where some big changes are unfolding—changes that result in risk. Meanwhile, risk fuels performance. How to strike the right balance? Those that can remain secure, vigilant, and resilient in the face of healthy levels of risk can gain a competitive edge.

There are two critical dimensions to the issue of cyber risk in service delivery. First, there is amplified risk that comes from shifting how, where and by whom services are delivered. But also, cyber risk management is emerging as a core, necessary service to the organization—just like Human Resources (HR) is a service, or Finance. What’s more, cyber risk management has deep financial, regulatory, and operational implications. In this issue of Connectors, we’ll examine these dimensions.
01 Pinpoint the factors contributing to your cyber risk profile

**Big data, big problems**
As organizations become increasingly interdependent on critical services, the scale and location of data becomes more complex to manage. In a recent high-profile data breach, the Office of Personnel Management (OPM), a large government agency responsible for soliciting and protecting a tremendous amount of sensitive information on behalf of other governmental departments, was compromised on a massive scale. Partly because of the sheer scale and volume of information held by OPM, it was difficult to zero in on which data types were the most important. Further, the data was scattered across servers hosted by other organizations. While the sensitive information clearly required an elevated approach to security, in the end, that was exactly the data that was compromised—along with many other types.

**Issues go beyond compliance**
Whether it’s a retail organization concerned about credit card data standards, a medical device company working to remain Food and Drug Administration (FDA) compliant, or a bank striving to protect customer account data, compliance is a big issue in cyber risk management. When these organizations shift service delivery to centers or offshore, compliance can be an issue—one so big, in fact, that it can obscure other important cyber security issues. For example, companies may be so focused on European Data Protection compliance that they fail to evaluate threat actors, or overlook options such as cyber insurance.

**What’s important?**
You may be surprised
“Protect the crown jewels.” It’s smart advice for anyone working in the realm of cyber risk management. But for company leaders accustomed to reading about high-profile data breaches in the news, it can be easy to assume that their own data is unimportant, much less determine which of it is most important: “We run a mining company—who on earth would be interested in our data?” Yet losing the availability of quality-related data on a hosted or outsourced system has the potential to create supply chain havoc and disrupt cash flow. The key is to consider not only which data might be useful to outsiders, but which could cause the most disruption if it were unavailable for some reason. It’s not as simple as it sounds, which is why there are a number of exercises routinely used to identify and rank data by its importance.
It’s about intelligence— not just control
In the face of new opportunities like those introduced by service delivery transformation, it’s tempting for leaders, such as Chief Information Security Officers (CISOs), to simply shut down pathways that are seen as particularly risky. This approach is basically a way to exercise control, often at a time when leaders need to instead be opening the door to more innovation and increasing speed to market. At times like these, CISOs should be working with their business counterparts to develop more risk-intelligent management protocols.

“Yes, and...”
In reality, many business users will end-run the rules in order to take advantage of new capabilities, raising rather than reducing the cyber risks involved. Innovation often outflanks policy. Cyber risk management leaders have to figure out ways to say “yes, and...” rather than “no”—particularly in the rapidly evolving space in which core services are delivered to the business.

Real consequences
In the midst of a massive acquisition, a global pharma remained laser-focused on maintaining system validation compliance with FDA guidelines on day one. On the first-day go-live, the company was indeed compliant—but it soon realized that it had exposed certain non-regulated assets to a considerable amount of risk. And this wasn’t just vulnerability to external threats. Along the way, the integrity and availability of operational and intellectual property information was compromised—no small issue for pharma companies, which depend on intellectual property as their lifeblood.
03 Practice cyber risk management in tandem with secure service delivery

Identify exactly how specific business goals are contributing to risk
What cyber risks are generated by your business objectives? Is a rise in business partnerships contributing to greater risks to confidential information? Are offshore centers in limbo due to the constantly shifting cross-jurisdictional data transfer environment? If third parties are handling critical information, are you exposed to a lack of contractual protections? Questions like these can help you anticipate your adversaries, identify which assets they’re most interested in, and which tactics they may use to exploit your vulnerabilities.

Deliver cyber as a service
Either through a shared services approach, or through outsourcing with a managed service provider, delivering cyber security as a service can ultimately lower your capital requirements and operating costs. Just as important, it can also expand your capabilities and shorten response time in the face of cyber events. Selecting and operating alternative delivery models for information security can hold significant value—and should be evaluated as a potential foundation for your security strategy.

Be realistic
Let’s be honest: it’s impossible to stop all cyber attacks. A more reasonable goal is to focus on reducing the impact of breaches when they hit. First, be secure: Protect critical assets against known and emerging threats. Be vigilant: Reduce detection time and develop the ability to detect the unknown. And finally, be resilient: Strengthen your organization’s ability to recover when an attacker makes it through your defenses.
Let’s talk

To transform your business, transform your service delivery model
Cyber security is a defining business issue today—and a key component of service delivery transformation. If you want to learn more about ways to stay secure in the face of transforming your global services, outsourcing, or shared services, we should talk.

Learn more about Deloitte’s Service Delivery Transformation practice

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2017 Deloitte Development LLC. All rights reserved.

Contacts

Jean White
Principal
Service Delivery
Transformation Leader
Deloitte Consulting LLP
jwhite@deloitte.com

Dave Smith
Principal
Deloitte Consulting LLP
davesmith5@deloitte.com

Dan Kinsella
Partner
Deloitte & Touche LLP
dkinsella@deloitte.com

Brian Claire
Principal
Deloitte Tax LLP
bclaire@deloitte.com

Cyber Risk Services contact

Edward W. Powers
National Managing Principal
Deloitte Advisory
Cyber Risk Services
epowers@deloitte.com

Authors

Sundeep Nehra
Principal
Deloitte Advisory
Deloitte & Touche LLP
snehra@deloitte.com

Steven Darroch
Senior Manager
Deloitte Advisory
Deloitte & Touche LLP
sdarroch@deloitte.com