StrategicCFO360 | tcs TATA CONSULTANCY SERVICES

CYBERSECURITY

Identifying, Managing and Mitigating Your Risk

> "The risk is real. Take a good hard look at your business continuity plan—specifically your disaster recovery plan."
>
> —Robert Watson, Engagement Director, Consulting and Service Integration, Tata Consultancy Services

From phishing attacks and malware to data leakage, the pool of cybersecurity risks is vast and ever growing. Along with greater efficiencies and revenue growth, each new way of leveraging technology or enhancing connectivity with employees, suppliers and customers brings additional vulnerabilities. Cybersecurity concerns are also complicating deal-making, as rigorous cyber risk assessment becomes a standard component of due diligence during IPO and M&A activity. CFOs and finance executives who gathered for a recent roundtable discussion on cybersecurity described grappling with the need to identify, assess and manage a vast array of threats coming from multiple directions.

At Westfield Capital, moving to cloud-based services has CFO and Chief Compliance Officer Kathryn Kearney concerned about the possibility of exposure through one of its partners. "We do vendor due diligence, but it's very difficult contractually to protect ourselves as we shift some of our in-house operations to the cloud," she said. "And if a client calls us when there's a security issue at another company and asks, 'Are you exposed to this?' we need to have an answer."

"The downstream and upstream risk coming from third parties is a very big deal," agreed Robert Watson, engagement director in consulting and service integration, Tata Consultancy Services, who urged companies to consider conducting a risk assessment and working with potential partners on mitigation efforts early in the partnership engagement process. "Often, the people writing the contracts don't even know the controls that need to be written into them to effectively ensure compliance. So, make sure your partners understand where the data crown jewels are and what controls need to be in place so that they can prove to you that they can ensure compliance."

Specialist data providers can help companies vet their supply chain for vulnerabilities, added Vikas Gopal, CFO advisory practice, Tata Consultancy Services. "They look at the entire ecosystem—not just your direct supplier, but that supplier's supplier's supplier. So, they actually build a complete map, quantify the risk exposure from failure at any point and give you a risk score, almost in real time, that can help augment your internal decision-making."

Vetting Partner Vulnerabilities

Generally, large-scale providers like Amazon, Google and Microsoft invest heavily in controls. However, greater scrutiny in assessing protective measures may be called for at the mid-tier level—which can be challenging for companies that lack the internal expertise to scrutinize providers for security holes. When manufacturing company Trussway was approached about transitioning to new equipment for its private cloud, the company bridged that gap by asking competing providers to assess potential weaknesses, recounted CFO John Tunison.

"They're always happy to tell us all the things that are wrong with their competitor," he said. "We also used what I'll call a neutral third party—an outfit that helps us with our network administration. They're knowledgeable in that area but had no skin the game because they weren't going to take over our hosting."

At KPFF, CFO Nikhil Kalghatgi reported taking a similar approach by hiring a virtual CISO company charged with identifying and mitigating risks. "We have a very qualified IT team, but this is not their area of expertise or their full-time job," he said. "So, we hired this company—not an individual because we wanted some redundancy—to stay abreast of what's going out on there in terms of risk and make sure they're keeping us honest."

While tapping outside expertise, tools and systems is helpful, the options can also be overwhelming, noted Jason Fowler, EVP and CFO of ACCESSbank. "One of the challenges we're facing is how many belts and pairs of suspenders do you put on? You hire a company to provide a service, then you hire another company to check their work. Then you feel that you have to hire another company to doublecheck that work. At what point do you start worrying about how much you're spending?"

Setting a Cybersecurity Spend

Broadly, companies devote approximately 1.8 percent of revenue to the four dimensions of cybersecurity—labor, technology, infrastructure and contracted elements or managed services. However, the figure varies widely by industry, and by company. The investment in cybersecurity should not only be tailored to a company's potential risks but also mirror the value and importance of its infrastructure, from financial systems to operational technology networks.

"A data-intense business will have a higher risk of impact than a company in a material production-based industry," explained Gopal, who added that risk appetite factors heavily in most companies' protection budgets. "You can invest a lot, you can invest some, or you can hedge with insurance, it's all a matter of how much downside protection you want to cover and how you want to go about it."

In weighing risk management options, it's important to be aware that insurance coverage doesn't cover reputational damage and may exclude pervasive types of attacks, such as ransomware, or require specific security measures to be in place. "We're in mid-policy renewal now and we're finding that some insurers won't even talk to you if you don't have enhanced protection, things like multifactor authentication and endpoint detection monitoring, in place," said Tunison. "One of the things driving our most urgent action right now, is doing what's necessary to make sure we can have cyber coverage while also trying to develop that longer-term plan and get ahead of the curve."

The prospect of opening the door to potential data breaches and/or what it might cost to prevent them can breed reluctance to embrace digital transformation. At Industrial Management & Training Institute, CFO Kim Nguyen hopes to bring an organization still relying on paper-based record-keeping into the digital age but is leery of the possibility of putting sensitive student data, such as social security numbers and transcripts, in jeopardy. "What can I do to have peace of mind that if we move to the cloud, everything will work?" she asked. "If we get attacked and lose access to student data, it will affect our daily operation."

The risk is real, responded Watson, who suggested taking a proactive approach to mitigating risk by focusing on building resiliency, or the ability to recover swiftly in the event of a cyber event. "Take a good hard look at your business continuity plan—specifically your disaster recovery plan," he suggested. "Have you invested in it? Exercised it? Make sure you have those data resources in other places so that you can restore what you need if you suffer a loss or get hit with a ransomware attack. You want to do everything possible to make sure that you're prepared."

Ensuring compliance with a widening array of data privacy requirements is also becoming critical, particularly for companies and organizations that collect sensitive data. Already, companies must meet a wide range of requirements, from local regulations like California's data privacy law to global polices like Europe's GDPR—and additional regulation, including measures from China and India, are in the works.

Step Back to Move Forward

At many companies, finance chiefs are front and center in meeting these cybersecurity challenges, weighing in not only on how much to spend but what types of systems and security tools to invest in. "We're small enough that I'm actually driving a lot of it," said Tunison. "One of the things I'm wrestling with is the need to step back and create a systems roadmap for where we want to be in 36 months. Where do we have nothing at all and are starting from scratch? Where are we just upgrading or migrating? That's my objective over the next six months before I start selecting software and vendors."

Fowler focuses on combatting two scenarios: an event that prevents the company from accessing its own data and a breach that compromises the privacy of its customers' data. "We have good systems in place with regard to backups, so that's going to be painful, but not as painful as our customers' information getting out the door," he said. "What keeps us up at night in terms of risk is our staff and the risk of someone clicking a link and letting the attackers in."

Ultimately, risk assessments that identify points of vulnerability that can lead to cyber events and quantify their potential costs are a crucial step toward mitigating threats. "Knowing the problem is 80 percent of the solution," said Gopal. "The more internal awareness a company has of its areas of risk—by employees, the board, through the organization—the better your chances of developing the ideal mix of safeguards, resiliency plans and coverage."

The investment in cybersecurity should not only be tailored to a company's potential risks but also mirror the value and importance of its infrastructure, from financial systems to operational technology networks.

StrategicCFO360

a Chief Executive Group community

StrategicCFO360 is the community powered by Chief Executive Group, publishers of *Chief Executive* and *Corporate Board Member,* designed to provide senior finance executives with the tools and insights they need to succeed as strategic leaders. StrategicCFO360 delivers informative webinars, timely research, dynamic conferences, peer-driven roundtables and the exclusive, one-of-a-kind CFO Network. Learn more at StrategicCFO360.com.

TATA CONSULTANCY SERVICES

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India. www.tcs.com