Compliance: Don't let IT be your Achilles' Heel

by Daniel Schneider

Business Development Manager Hybrid IT Managed Services

Ensuring that your organization is compliant means managing everything you do and every technology you use with a close eye on compliance rules and regulations. It's a big task, says Fujitsu's Business Development Manager Hybrid IT Managed Services Daniel Schneider, and is best achieved with the right partner.

Referring to an ancient Greek myth might seem like a strange way to introduce the subject of compliance, but I'm not the first to do it. Far from it. If you look back, there are many references to the story of Achilles' Heel in all kinds of professional contexts, from legal papers to discussions on construction, mining, and just about any other business. It's an enduring myth because it warns us all that there may be one thing – one tiny vulnerability – that could bring everything down.

When it comes to cloud, the story is instructive. The incredible volume of data that flows across networks – between employees, to and from customers, suppliers, partners, and different entities public and private – has prompted governments and authorities everywhere to strictly regulate its exchange, storage, and use. Europe's GDPR is a prime example. It, like all the other similar regulations, can punish non-compliance with substantial fines. And financial pain is usually compounded by reputational damage. Together, they can be fatal to the health of any organization.

You can choose to see compliance as a chore and a cost, or just as a nuisance. Thankfully, not many organizations do. Most organizations are working to win and maintain the trust of their customers and employees as trust is the most important currency. It's not that much sticking to the letters of law. And it's not just data that's at issue; how systems are used to move money from one place to another and one person to another are also covered by a range of regulations to stamp out fraud, money-laundering, and bribery. Technology touches everything an organisation does: data, money, and even health and safety.

Any gap in the system, any error (human or technical), any misuse of a technology or malicious attack, can lead to a breach and a big headache for the entire organization. That's why organizations are focusing heavily on compliance. It's a necessary investment in customer, partner, employee trust and time consuming, but the cost of negative exposure, lawsuits, and fines could be catastrophic. Fear of compliance issues is, in some sectors, slowing the move to the cloud. The financial sector is especially vulnerable. A recent report showed that the sector was hesitant about moving its data and payment systems onto cloud platforms.   Though it did reveal that there was a growing understanding that a hybrid approach should be a preferred option. The use of cloud and cloud

service providers [CSPs] offers a significant uplift in resilience and security compared to banks' on-premises environments. [1]

So, what's the answer? Do you need to employ a team of compliance specialists to search every inch of your business for possible vulnerabilities (that vulnerable heel) and check every action to see if it might just be in breach of any one of thousands of regulations? At Fujitsu, we don't believe you need to do that. We have deep experience in not only ensuring our own compliance in accordance with rules and regulations of various states, but also taking this burden away from our customers.

Not properly used technology or technology used by inexperienced users might be the cause of many vulnerabilities – but properly utilized technology by expert users is also the answer. Fujitsu's Cloud Management Service is all about the detail. We work closely with our customers' internal compliance teams to ensure that the right guidelines and guardrails are put in place across their systems and networks. Naturally, the responsibility for the compliance and security of the cloud platforms they use lie with the providers, but we ensure that there's a system-wide focus on compliance that extends to every department, team, and technology across the entire ecosystem.

Paying attention to upgrades, patches, and how new technologies are integrated with existing ones, is vital. We manage all this. We do the things that seem mundane but might represent a significant vulnerability if left undone. We set external guidelines to match your own. And we make good use of AI to automate protection (with self-healing properties to ensure no gap is left unattended). That means you can focus on what you do best. Of course, nothing is 100% secure, but if every regulation is followed – and can be *seen* to be followed – then you can stay on top of compliance.

At Fujitsu, we believe that compliance is not a burden. It's an investment and actually a key element in achieving resilience, agility and trust (see my other blogs). You can't focus on innovation if you're always looking over your shoulder, especially at a time when cybercrime is rising fast. Enabling your data to flow freely and securely and in complete compliance with ever changing global regulations frees your people. They can do great and new things to delight your customers and stakeholders. We can't promise immortality, but we can ensure there's less chance you'll suffer from an Achilles' heel.

Find more information about Fujitsu's Cloud Management Service here.

---

[1] https://www.computerweekly.com/news/252507100/Regulator-concerns-about-resilience-and-security-could-slow-cloud-adoption-in-financial-services