Follow the bouncing compliance regulations

Ever-changing rules, corporate landscapes, and supply chains put compliance mandates always in play. Juggling those variables make the CISO's compliance requirements a moving target. Evan Schuman explains.

When wrestling with compliance requirements, CISOs often feel like like they are a performer in the middle of a three-ring circus, rapidly trying to juggle sharp knives. No matter how fast or perfectly they juggle, there is an assistant, or in this case regulator, behind the curtain constantly throwing out more and more knives, each one larger and more deadly. But instead of knives, the real enterprise CISO juggling acts are spheres of compliance.

The horror of cybersecurity compliance can be viewed as two or three rotating spheres, each orbiting around another.

The first sphere represents the rules, the constantly morphing set of geographical and vertical compliance requirements from around the globe. Sometimes these rules and regulations can contradict one another, adding an additional layer of headaches and challenges for the CISO.

The second sphere is the enterprise itself with its own compliance landscape changing weekly. Changes might come as the company launches new products, changes its business practices, or moves into and out of different geographical areas and verticals (perhaps through mergers, acquisitions, and division sales), which itself can change the compliance rules that its CISO must address.

The third sphere, which applies to a smaller percentage of companies, includes a company's customers as they move in and out of different verticals and locales and what data they choose to store with you. For example, if a retail market chain client of a hosting company were to acquire a drug store that held customers' personal health information and started storing that data on the host's site, that hosting service would be required to meet a variety of different compliance requirements that it previously might not have been required to meet. If the client does not inform the hosting provider of the new data stored on its servers, the provider could be out of compliance and vulnerable to lawsuits.

With apologies to IBM, one can think of this as compliance's Sphere, Uncertainty and Doubt — the SUD factor. The task of tracking where all spheres are at any one point faces a number of hurdles, including internal politics (another business unit not promptly sharing plans that will impact compliance), conflicting legal interpretations of both rules and contract language with contractors, and technological obstacles, especially with cloud, mobile and internet of things (IoT) environments.

Not all compliance executives surrender to this compliance insanity, although many are tempted.

"I choose not to focus on the compliance nightmare. Go ahead and have your 30 seconds of self-pity and move on. You're not going to beat Goliath here," says Christopher Rogers, the deputy CIO and global security officer for consulting firm Sykes. "If you take

OUR EXPERTS: Compliance

David Deckter, partner, Edgile
Doug Graham, chief security officer, Lionbridge
Thomas Johnson, CISO, ServerCentral Turing Group
Christopher Rogers, deputy CIO and global security officer, Sykes
Eric Sampson, senior manager, Schellman & Company

94%

Respondents who say cyberattackers have an advantage over defenders

– ESG

compliance to [mean] just checking the box, well, it's one step above negligence but it gets you the certificate."

"We get so many requirements, we can't make sense of them," says Doug Graham, CISO and chief privacy officer for AI testing at the translation firm Lionbridge Technologies Inc. of Waltham, Mass.

Doug Graham, chief security officer, Lionbridge.

Graham points to the European Union's General Data Protection Regulation (GDPR) as an example. Although the EU has published a version of GDPR, that might well not be the rules with which many companies will have to comply. The EU is giving every member country the ability to modify GDPR however it chooses. That means that, as a practical matter, companies will have to comply with as many versions of GDPR as there are EU countries where it has employees, contractors, or customers. Officially, there's no guarantee that every EU country will opt to make changes, although many might select that option.

> "If you take compliance to [mean] just checking the box, well, it's one step above negligence but it gets you the certificate."
>
> *– Christopher Rogers, deputy CIO and global security officer, Sykes*

"There are clear areas where countries are encouraged to go their own way," Graham says, adding that there are also situations where the baseline EU flavor of GDPR will be dominant. The best route to try and keep up, Graham says, is to decentralize the compliance officer role and embed compliance specialists within as many key business units as practical.

Many companies on the Fortune 500 list and their comparably-sized private counterparts are gradually shifting an increasingly large percentage of their data off premises and into the cloud. It is not surprising that the cloud poses some of the most curious compliance challenges.

One of the more daunting challenges is that cloud platform staffs — especially the megacloud service providers where a large percentage of Fortune 1000 sized-companies purchase services — will make multiple settings and configuration modifications daily without informing corporate tenants. Cloud providers likely will stress that they are compliant with a wide range of geographic and vertical requirements, and this is typically true.

However, the cloud vendor being compliant with the Payment Card Industry Data Security Standard (PCI), *Health Insurance Portability and Accountability Act* (HIPAA) or GDPR is very different from offering an environment that guarantees that same level of compliance for tenants.

Each tenant has a different compliance landscape so each tenant's CISO must make their own compliance determinations. That means that these megacloud providers cannot know how even a minor, seemingly innocuous setting change could impact the compliance efforts of a Fortune 1000 tenant.

One possibility is that one of these cloud companies might opt to position themselves as the compliance-friendly cloud provider as a competitive differentiator. They would then compile a daily list of every setting/configuration change from that day and share it with all tenants, either via an email blast

54%

Respondents who say they have been subject of a DDoS attack

– Morning Consult

or having that day's document of changes accessible via a secure page on their site.

Even if a major cloud vendor opted to share all that data, there still is the issue of every change made by the cloud vendor's many subcontractors, including backup and disaster recovery services. In order to pursue full compliance, every tenant would also need to know every change made by every subcontractor. And so, as each modification in the supply chain becomes just another line item in this ever-expanding nightly list, the nightmare gets worse.

David Deckter, partner, Edgile

The Janus effect

Ancient Romans might well have considered dealing with today's compliance as the Janus effect, named for the god of doorways, beginnings and endings. Rogers says that he often finds cloud provider compliance can make compliance far more difficult given communication issues, but that they can also make compliance easier given the superior security mechanisms many of the largest vendors have in place.

Rogers notes that even with notice from vendors change is never easy. "Microsoft Azure gave us about an hour's notice that they were going to do some significant patching. There was no request that we approve it, nor any understanding of how long it would take. It was 'Here it is. You need to deal with it.' I am losing control of my ability to directly influence my environment," he says.

> "The right to audit clause is one that is frequently missed."
>
> – David Deckter, partner, Edgile

"We ask our cloud vendors where they can provide [compliance] attestations and where they can't," Rogers says, adding that he has seen some improvements over the years. "In the early days of Office 365, we couldn't get attestations from Microsoft."

As for the suggestion that a cloud vendor might share more details about their environments, along with those of third parties they have retained, Rogers was supportive but not optimistic. "The request is not unreasonable, but the reality is that it is not going to happen, unless you're a Netflix. It would mean that every time they patched, changed connectivity, [it would have to be reported to tenants]. These companies are massive and to just share the standard operational details, the level of small and medium changes are going to be almost constant."

Rogers' quip about Netflix reflects the practical concern that many security specialists share: Negotiating with cloud vendors is a matter of clout and size. Is the cloud vendor larger than the customer? How much does the cloud vendor want that particular piece of business? The idea that a cloud vendor might share this very lengthy list of details with every enterprise tenant is highly unlikely, he believes.

Managing responsibilities

Security compliance specialist David Deckter, a partner with the Edgile consulting firm of Austin, Texas, where he leads Edgile's governance, risk, and compliance practice, suggests CISOs simply list out everything handled by the enterprise versus the cloud vendor — and all of the cloud vendor's contractors and subcontractors — in order to have a better sense of who is supposed to handle what.

$4M

The average data breach costs $3.92 million

– Ponemon Institute

"Define the stack, and by stack, I mean all the different topics that will come up, including network change management, network configuration, firewalls, operating system config, OS patches, etc. You define your full stack and that is your entire universe," Deckter says. "I, as the tenant, have control over only these subsets. And here's what the vendor manages. I am forced to rely on the [cloud] SOC (security operations center)."

Eric Sampson, senior manager, Schellman & Company

As for sharing all the specific changes, Deckter also finds that highly unlikely. He cites Microsoft Exchange email as an example. "Do you think that Microsoft is going to let one of their customers fiddle with the firewall rules and the network configurations?"

The suggestion is not changing anything, but merely being aware of what has changed.

"If Amazon makes a change with a subservice organization, are they going to report on it? I'm not sure they would," says Eric Sampson, senior manager of Schellman & Company, a security and privacy compliance assessor.

Another critical compliance issue with cloud platforms is the cloud subcontractors specifically. "In the banking world, you need to know who your fourth parties are," Deckter says, in order to comply with the Office of Foreign Assets Controls (OFACT) sanction list. "Perhaps you can't do business with Venezuela or Syria. You need to understand the geography of where your work is taking place," he says, pointing to various data sovereignty issues.

"Cloud providers have global operations. You might have contracted with company X with a U.S. domicile [but] they have operations and staff sitting offshore. Who is doing the administration of your system? Where are these people? And who have access to your environment?"

Deckter argues that many CISOs are not negotiating for the appropriate rights in cloud contracts, such as disclosing fourth-party details. Another Deckter concern is the right to audit and what exactly the cloud vendor considers to be an audit.

"The right to audit clause is one that is frequently missed," Deckter says, pointing to third-party review of all service providers. "That's the first thing you bump up against." He notes that the cloud vendors will say to CISOs, "Sorry. Go away. You have no right to audit." More typically, however, Deckter says he sees enterprise CISOs being given contract terms allowing for the right to audit just once a year. That is where the definition of what constitutes an audit comes into play.

> "Selecting an audit firm may have been a lowest-bidder-wins endeavor in the past, but now it is seen as more of a partner to help navigate compliance, determine applicability, and define a new control structure."
>
> *– Thomas Johnson, CISO, ServerCentral Turing Group*

In a scenario Deckter paints, a business unit manager asks the cloud vendor for a document, such as a certificate of insurance. Then the CISO, perhaps a month later, goes to the cloud vendor and asks to do the once-a-year audit and the CISO is rebuffed. Deckter says the cloud vendor might tell the CISO, "Try next year. You've exhausted your right to audit. You're done. Come back

38M

Number of breached U.S. medical records for the first nine months of 2019, the second-highest total in the past six years.

– HIPAA Journal

next year." That, he says, "trips people up as well."

So just what constitutes an audit? Does an audit mean third-party penetration testing? An on-site unannounced inspection? Or is any request for any document an audit? Part of that definitional negotiation could be a number negotiation. For example, if the cloud vendor is insisting on a definition that states an audit is any data request, the CISO might reply: "If you won't change that definition, then increase the number of annual 'audits' to 15. Your choice."

Deckter notes there are usually multiple departments that can make data requests of the cloud vendor, including IT, privacy, ethics, compliance, and legal; there needs to be a process to make sure no one unintentionally uses up the enterprise's number of contracted requests. For example, if a procurement department asks for something from the service provider and the request was not coordinated with other departments, it could block everyone else from making a request to the provider, Deckter says.

Thomas Johnson, CISO, ServerCentral Turing Group

Another compliance problem that can catch CISOs unawares are cloud vendor issues with their inventory. Sometimes, he says, "[cloud vendors] don't know what is on their production network. Things that are on third-party environments and the third-party doesn't know what they are," Deckter says. CISOs must set a percentage-based tolerance of unknown assets and Deckter recommends that the cap be no higher than one percent.

Deckter says he has run into situations where the percentage was much higher. He says that he once said to a cloud vendor: "You're telling me that you don't know what is in 30 percent of your assets?" It might be that 5,000 devices on the cloud's network are not listed in the inventory. "'I don't have the MAC address or IP address in my list' means those assets are probably not being patched [or tracked by] vulnerability scans because [the cloud vendor] doesn't know about it. It should be no more than one percent. No one thinks about this. You need to set a key performance indicator of one percent tolerance of unknown assets on the network."

Wrong place, wrong time

There are pros and cons about what size cloud vendor an enterprise should select; it depends heavily on the nature of the systems being defended and the size of the enterprise. A Fortune 100 company might have the clout to get far more concessions in a negotiation, but a smaller enterprise might still need the stronger protections from a larger cloud provider.

But, Deckter says, sometimes a large cloud provider can invite attacks from criminal elements that might not have otherwise targeted a specific enterprise. "There is a concentration risk due to the fact that when China comes after Amazon or Microsoft or Google, I am now part of that ecosystem. [China] is not necessarily coming after me. You are now part of an extremely high-profile environment," he notes.

That said, Deckter adds that the security from the larger players is often worth the cost. He believes that, in most cases, the reason smaller cloud firms are less expensive is because they are not delivering the same security services as their larger competitors.

Often one of the key negotiated security compliance requests from CISOs for cloud vendors is penetration testing. If pen testing is allowed at all, it generally must be announced and done against a non-production server.

61%

Percentage of EU-based organizations that reported a data breach in 2019

– Hiscox Cyber Readiness Report 2019

Otherwise, there is a legitimate risk that the testing will appear to the cloud vendor as a real attack with networks potentially shut down, law enforcement alerted, and other problematic triggers enabled.

Whether cloud vendors will permit even announced pen testing is an open question. Some compliance specialists say it is an important component to request. However, the rules of engagement must be defined. How frequently can you test, if any areas are off-limits or if specific servers are designated for such tests, and what the tester is permitted to do, for example. Smaller cloud vendors often will be more open to granting such requests.

Deckter cautions that there are serious reasons to avoid pen testing. "Let's say that you got Microsoft to agree to a pen test from you and you're doing the pen test [when] you [accidentally] take down that operation, you took down other [Microsoft clients]. What's your liability?"

Such an example demonstrates why providers generally require any pen tests to be against non-production systems so that a miscue cannot impact other customers.

Deckter offered an example from his early career. He was working for a company with compliance obligations and he was scanning a field mill. It turned out that the pen testing caused operations in Indiana to shut down "because [the] passive scanning to determine if we had ports open took down both of the machines providing steel. It didn't exploit anything but a faulty TCP/IP stack, but it caused it to crash."

Vulnerability testing might be more acceptable to the cloud provider than even passive pen testing, Deckter says, especially considering that the larger cloud networks' systems run through other countries. "It isn't going direct only to that cloud environment. You might have to pass through AT&T's networks and other networks and you may inadvertently take their stuff down. Do we have adequate insurance?"

Others point to cloud-related compliance issues, which reflects less of a concern about the cloud data versus on-prem data and more how to bridge the combination of the two, the typical hybrid environment that almost all Fortune 1000 enterprises utilize.

> "Over the years, particularly in the area of PCI compliance, multiple clients I have worked with indicated that their previous auditors had passed them in meeting compliance when they should not have passed."
>
> *– Eric Sampson, senior manager, Schellman & Company*

"In this day and age of containerization, cloud technologies, and on-demand compute, it is hard to interpret/decipher how some of these compliance requirements — designed for traditional on-premises infrastructure — fit into the cloud ecosystem of products," says Thomas Johnson, CISO at Chicago-based cloud consulting firm ServerCentral Turing Group.

"What's even worse is being coupled with an auditor/audit firm that is not well versed in the technology and is accustomed to traditional technologies. Selecting an audit firm may have been a lowest-bidder-wins endeavor in the past, but now it is seen as more of a partner to help navigate compliance, determine applicability, and define a new control structure."

Shellman's Sampson argues that many CISOs pay insufficient attention to whom they hire as auditors or assessors, often only finding out late in the game the auditor cannot handle the technology at issue. Sometimes, that is the result of not paying attention, but it is also often driven by a false sense of economy where companies want to spend as little as possible on an assessment. Sometimes the lowest bidder is

#1

Belgium was the most heavily attacked EU country in 2019 and reported the highest number of supply-chain-related attacks

– Hiscox Cyber Readiness Report 2019

often the least qualified or just the easy graders.

"Over the years, particularly in the area of PCI compliance, multiple clients I have worked with indicated that their previous auditors had passed them in meeting compliance when they should not have passed," Sampson says. "I had one client who asked us to come in and do a PCI readiness assessment in which we pointed out many areas of non-compliance.

"Upon learning what it would take to become compliant, they said they weren't ready to address the identified gaps and went to an audit firm that wasn't as scrupulous in their review and passed them on PCI compliance," he continues. "They said they'd come back to us when they were ready to have the 'real' PCI audit. 'Not every auditor is created equal' is an observation that there are auditors or audit firms out there who for whatever reason pass on compliance when they shouldn't.

"I would be speculating on the reasons why this is," he concludes, "but some reasons may be that auditors lack training and experience, audit firms lack proper quality assurance review procedures, or audit firms do not provide their auditors with sufficient time to properly complete their review, thus causing the auditor to pass on information being provided without adequately reviewing the information." ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at (347) 480-1749, or via email at david.steifman@cyberriskalliance.com.

67%

Respondents who will look to AI to automate IT processes intelligently

–ESG