The wacky world of GRC

Few areas of technology are as contradictory as governance, risk and compliance. A company might do everything to be secure yet still not be in compliance. Evan Schuman investigates.

For some, maintaining a focus on the governance, risk management and compliance (GRC) landscape is data security nirvana, the epitome of an ideally balanced data strategy. For others, it's a maddingly frustrating and impossible task where conflicting geographic rules and industry standards make strict compliance untenable and the attempt counter-productive. Just to make life interesting, it turns out that both these perspectives have a semblance of truth.

The most popular suggestion for GRC compliance is to focus on the intent of regulators and standards bodies – most of which base almost everything on security and privacy best practices – and not the letter of their edicts. Many regulators, auditors and assessors are much more forgiving when they see that someone truly is trying to deliver a safe and secure environment and avoiding the checkbox mentality approach. That said, "many" does not equal "all," which is why data security in 2017 is not for the faint of heart.

"There are absolutely directly contradictory and conflicting regulatory policies in global environments," says Joel Bilheimer, a vice president of cybersecurity at Pershing Technologies, a technology solutions provider based in Columbia, Md. "It is almost impossible to be 100 percent fully compliant all of the time. It actually is impossible, when you consider elements like training, personnel evaluations and day-to-day operations."

Bilheimer sees lots of major enterprises and "literally none of them are perfectly compliant. That is almost by design, by the design of the process."

Tim McCreight, director of advisory services at Above Security, a Calgary-based IT security service provider, argues that obtaining compliance for virtually every regulation is pretty tough. "We will never be completely secure or safe. The absolutes we never will obtain." Just don't accept the lowest bar of literal compliance, he says. But McCreight, a former CISO for the government of Alberta (Canada), says that all GRC is a balancing act. But the balance needed is not merely between different industry or regulatory requirements or even security requirements. Everything also has to balance properly with the needs of the business to generate revenue and profit and to even simply function.

For example, McCreight once tried lassoing in all of his enterprise's data to prevent unauthorized downloads and to simply have a more controlled list of data assets in his organization. That interfered with employees working offsite and it didn't go down smoothly.

He tried the brute force approach and blocked everything in terms of mobile and cloud that hadn't been authorized. It just riled

OUR EXPERTS: GRC

Doug Barbin, principal cybersecurity analyst, Schellman & Company
Joel Bilheimer, vice president of cybersecurity, Pershing Technologies
Bruce Bonsall, member of the executive faculty, Institute for Applied Network Security
French Caldwell, chief evangelist for MetricStream; former cybersecurity adviser to the White House
Dante Disparte, CEO, Risk Cooperative
Françoise Gilbert, attorney, Greenberg Traurig
Karl Mattson, CISO, City National Bank
Tim McCreight, director of advisory services, Above Security
Kenneth Pfeil, chief architect, TechDemocracy

GRC

$141B

Estimated worldwide spending on public cloud services in 2019.

– IDC

everyone. "I started asking people 'Why are you using a cloud provider?' Their answer was that they just had to get their jobs done. Users are like water: They will find the fastest way around something if you're in the way."

As for GRC adherence itself, McCreight says businesses need to triage what is essential for their own operations. "I have seen organizations get two out of the three done well. I think technology has moved far faster than our laws," he says. "As a CISO, if you have an understanding of the critical systems – where unstructured data could occur – you have a fighting chance to understand your risk."

Douglas Barbin, principal cybersecurity analyst, Schellman & Company

Bruce Bonsall, member of the executive faculty at the Institute for Applied Network Security (IANS), an information security advisory and consulting firm, and formerly CISO for MassMutual Financial Group, agrees. "You can be compliant and not be managing risk well, but if you manage risk well, you will end up being compliant."

French Caldwell, chief evangelist for MetricStream, a Palo Alto, Calif.-based GRC solutions provider, sees GRC differently and argues that all three legs are essential and, indeed, help to enable each other. "Without compliance, there is no governance. And without risk management, you really don't know how much compliance you really need. You can't do one without the other two," says Caldwell, a former Gartner fellow and vice president as well as adviser to the White House on cybersecurity.

Then there's privacy

A sometimes overlooked – or undervalued – element of GRC strategy is privacy. This is because, even though one sliver of a privacy strategy involves security – making sure, for example, that cyberthieves can't access personally identifiable information – much of it is handled by people, such as marketing managers, typically far removed from GRC efforts. Issues surrounding opt-in rarely involve CISOs or CIOs.

Depending on who is being asked, privacy is either a geographic issue or it's not.

Françoise Gilbert, an attorney specializing in global privacy and data security with Miami-based, international law firm Greenberg Traurig, argues that European executives see data privacy very differently than do their U.S. counterparts. "Under American culture, data protection means security. In Europe, data protection means privacy," Gilbert says.

Here again, Caldwell disagrees. Working with the White House on cybersecurity has given him a unique perspective. He says he has often heard the view from European executives that their American counterparts don't think about privacy. "You hear that in Europe quite a bit, but if you look at actual enforcement of privacy, U.S. [regulators] issue much heavier fines and more active enforcement," Caldwell says. In short, he argues that the U.S. has weaker privacy laws but stronger enforcement of whatever laws exist.

Caldwell's enforcement position doesn't necessarily contradict Gilbert's point that American executives tend to play down privacy issues. If Gilbert is right and U.S. executives do indeed give insufficient attention to privacy matters, that could explain more fines and more aggressive enforcement.

Caldwell says that the nature of GRC software today tends to exacerbate the problems. "If you're a GRC professional – an auditor, risk manager, compliance manager, or IT security professional – you spend much of your working day in front of a screen,"

#1

Security will displace cost and agility as the privary reason that government agencies move to the cloud.

– Gartner

he says. "Navigating enterprise software with cluttered screens and rows and rows of input forms is not going to drive the greatest productivity for the business."

Another veteran financial vertical CISO, Kenneth Pfeil, agrees that many of today's GRC compliance tools could use some serious updating. "Traditional GRC tools were designed at a time when the rate of change for controls, threats and regulatory landscape were, for the most part, pretty static and not very adaptable to significant change without shifting the whole risk measurement model," says Pfeil, who served as the CSO for MFS Investment Management and the CISO for Pioneer Global Asset Management before moving into his current role as the chief architect at TechDemocracy, a global cyber risk assurance solution provider, with U.S. headquarters in Edison, N.J.

"While things have gotten a little better, we will increasingly see change at a faster rate – due in part to things like advanced threats and actors, Internet of Things, country policy changes, etc. – in the future," Pfeil says. "Unknown variables are particularly challenging to compute risk and compliance against. I'm not convinced that GRC is a one-size-fits-all solution."

Bruce Bonsall, member of the executive faculty, Institute for Applied Network Security

Part of the problem, he says, is that CISOs and other data executives focus on what they can most easily see and count. "Most companies are not even aware of what data their third parties are aware of," Pfeil says. Instead, they tend to focus on a very short list of priorities: "What's going to get them fined, what's going to get them fired, and what is going to get them in trouble."

Or, more precisely, what those executives *perceive* to be the things that will get them fined, fired or in trouble. And that forces the security executives into predicting what Payment Card Industry Data Security Standard (PCI DSS) assessors, state or federal regulators, or auditors and their geographically distributed counterparts will consider to be important. With that diverse a group of potential regulators – with such differing goals, objectives and backgrounds – such predictions are almost impossible to get right for all of the potential requirements all the time.

To a huge extent today, companies are dependent not on the kindness of strangers as much as the security and privacy-sensitivity of partners. "Most enterprises have large networks of business partners and major in-business models that are heavily dependent on information technology," Caldwell says, "and today, IT investment means investing in third-party provided services and cloud-based solutions."

With these extensive networks of business partners, suppliers, IT services providers and cloud solutions, enterprises today have more critical dependencies on third parties than ever before, Caldwell says. "Business continuity doesn't depend just on your processes and systems working effectively, it also depends on your suppliers and IT providers. You are also exposed to the risks that your business partners and vendors are taking."

This forces a change of thinking, away from a compliance view and moving closer to the thief's view.

"Organizations need to build a compliance strategy not based on how the auditor is going to review it but how the cyberthief is going to infiltrate," says Douglas Barbin, a principal at Schellman & Company, a Tampa, Fla.-based data security and compliance consulting firm. "We see so many times people write policies and build a governance program for the auditors, but they need to build it for the true risk,

27%

Respondents who say they monitor their business partners at least quarterly for corruption.

– Dow Jones and Metricstream, 2016 "Global Anti-Corruption Survey"

penetration and vulnerability of the system."

Barbin maintains that companies must focus on the elements of GRC that most impact their companies and focus on those – along with generally trying to be as strong on security as possible. When auditors and regulators see that approach, as opposed to the ever-popular checkbox mentality, they will tend to be far more accommodating.

"It's impossible to meet every one, but you can meet major sets of requirements, whether that is the state of California or some sort of accreditation board," Barbin says. "Policies are built for compliance standards, but new technology and emerging technologies – such as IPv6 – are not being integrated. But they are threat factors."

Think ease and compliance, he says. Organizations may not support Windows 10, but employees are using it. New technologies are implemented in the environment before they are addressed in policies, such as BYOD [bring your own device] and MDM [mobile device management]. "The trend to corporate-owned assets to personal [assets] has been executed much faster than the GRC team can handle," Barbin says.

French Caldwell, chief evangelist for MetricStream

Barbin says that he agrees with attorney Gilbert that European corporate executives tend to take privacy more seriously. "In the audit world, we typically audit against commitment," Barbin says. "Privacy has always been one of those that is a little looser, less defined than security. Everyone does security. It's comfortable for everyone."

Leveraging software

One fan of leveraging today's GRC software options aggressively is Karl Mattson, CISO for City National Bank (CNB). He is based in the Los Angeles office of the American financial institution that holds $47 billion in assets and is a subsidiary of Royal Bank of Canada (RBC).

"Compliance is a complex area," Mattson says. "Regulators and states and national institutions are changing compliance all of the time." CNB's ultimate strategy, he explains, is to invest in GRC automation so that it can assess compliance once, and satisfy all control requirements.

"As new regulations are formed and compliance changes, we don't have to overhaul the entire system each time," he adds. "The complexity and diversity of regulatory and compliance requirements is a constant challenge. There are literally hundreds of frameworks and thousands of control elements. Are we missing something? How do we avoid being non-compliant? One of the key things we do is maintain relationships with our peers across the industry to share best practices and keep our fingers on the pulse."

Mattson says he has seen organizations do better with homegrown programmed versions of Excel and SharePoint compared with shrink-wrapped enterprise apps that are marketed for GRC compliance. That is because the off-the-shelf commercial apps are designed to cover a mammoth array of requirements, many of which might not apply to any one company. Conversely, the homegrown apps are likely going to cover everything that applies to that company and nothing else.

That means that company executives, in theory, should be able to have more faith in their versions. Unfortunately, Mattson says, many firms have unrealistically high expectations of the commercial versions, which in turn can cause problems.

But Mattson joins the club of CISOs who

12%

Government sanctions increased 12 percent from 2015, where 89 percent of respondents note it as the most likely trigger to relationship reviews.

– Dow Jones and Metricstream, 2016 "Global Anti-Corruption Survey"

sees legions of cloud-based companies as making compliance far more difficult, if not almost impossible. "The biggest challenge is how to interpret compliance requirements with third-party, cloud-based technology providers. We understand our control obligations for systems and data hosted internally, but how do we translate those requirements for systems and data that aren't hosted internally?" Mattson asked. "In addition, a huge issue for 2017 will be mobile systems security."

Sometimes, it's the public posture about a company's GRC strategy that can be a problem, suggests Dante Disparte, CEO of Washington, D.C.-based consulting firm Risk Cooperative. "In terms of information security, only the largest companies on the planet can meet the toughest standards," Disparte says. "IT security spend is often seen as a proxy for greater safety. This dilemma is creating a veritable feeding frenzy and a ballooning market, but it is not necessarily making organizations safer."

Kenneth Pfeil, chief architect, TechDemocracy

In fact, he says, this is gamifying the security business by putting an unsolicited target on the backs of companies that tout how impermeable they are.

Alas, the list of GRC trouble spots is practically endless. Gilbert singles out training challenges as one of her top fears. "There is simply not enough training," she says. "Some companies offer video briefings and then ask employees to check five questions and then you're done. This is not training. This is checking the checkbox."

CNB's Mattson complains about the lack of qualified people to even take that training. "Lack of talent is a big issue in keeping pace with ever-increasing industry regulations and requirements. The industry is just not producing enough high-caliber risk management specialists who understand this space," Mattson says. "Organizations are forced to do a lot of in-house, on-the-job training. There's a lot of understandable pressure to keep pace with compliance, but we need more talent to do it effectively."

Mattson also laments that many of his employees seem eminently trickable by con artists, identity thieves and cyber attackers. "One of the areas I'm most surprised by is the prevalence of spear-phishing attacks and that organizations can still be compromised. The success rate is greater than you'd expect," Mattson says. "We invest a lot in technology and training elements to prevent these attacks, but the creativity of our adversaries is impressive. Even rudimentary attacks can be successful as the human element still plays a role."

Then there's every security manager's favorite GRC boogeyman: IoT devices. "With IoT, it's going to blow up," Pfeil says. He questions how car makers who are exporting their vehicles are ever going to protect IoT elements. "We need to have a die date for devices. Otherwise they'll be connected forever and never get updated."

But if die dates exist on cars, that is going to mean that important operations will simply stop functioning. Try explaining that when selling a pre-owned vehicle.

Pfeil also questions the ability of these devices to employ robust authentication. That's critical because these device manufacturers often stress that the devices will only accept, for example, firmware updates from the manufacturer.

Set aside how well an overseas manufacturer can be trusted. The truth of the matter is that such an IoT device will accept anything labeled firmware from anyone who claims to be the manufacturer. Which begs the ques-

30%

In a survey of corporate boards of directors, only 30 percent says they are "Excellent" at quantifying risks.

– PwC

tion: "Just how effective is this IoT device's authentication system?"

Bonsall also expresses worries about IoT. "It takes awhile to figure out what kinds of abuse things will have. This stuff is moving so fast it's hard to keep up with it," he says.

So can an effective GRC strategy deal with all of these elements globally or is the best approach a "pick your shots" strategy? The answer comes down to the nature of your business, your customers, your partners – especially your partners – and the risk tolerance of your executives and the industry regulators in your space.

A hospital dealing with requirements of the Health Insurance Portability and Accountability Act of 1996 – commonly called HIPAA – might indeed need to have a stricter GRC strategy than a manufacturer with twice the revenue but no HIPAA involvement. Geography is also a key determining factor. That's not merely where you have operations and personnel, but where you have customers and distribution, OEM and design partners.

Are we saying that the country base of a group of outsourced coders should really dictate an enterprise's GRC strategy? Yes. Does it? It depends. Welcome to one of the most consistently contradictory set of rules in the world. ■

For more information about ebooks from SC Media, please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

93%

of organizations surveyed are running applications or experimenting with infrastructure-as-a-service.

– RightScale, "2015 State of the Cloud Report"