Is your governance, risk and compliance plan up to date? Compliance rules change often and managing risk is like herding cats.
With so many major pieces of the security puzzle in flux, how can you be sure you’re harmonizing your business practices? We break down the top priorities of GRC. Karen Epper Hoffman reports.

Six years ago, Mark Zuckerberg, founder of Facebook, said, “The biggest risk is not taking any risk. In a world that is changing really quickly, the only strategy that is guaranteed to fail is not taking risks.”

Most entrepreneurs would agree that statement is still true: No organization nowadays can thrive, or even survive, without taking on some amount of risk. However, senior executives, especially those tapped to manage IT security, would also point out that the real challenge is knowing how to manage that risk, implementing the proper governance over their people and processes, and making sure they are compliant with all the necessary and ever-changing regulations and guidance. That, the experts say, will be the challenge that will ultimately separate the businesses that lead their sectors from the ones that end up shamed in the headlines or lagging behind their competitors.

Governance, risk management and compliance (GRC) is therefore becoming an increasingly key component for cybersecurity – and business management and strategy in general – as organizations assess the potential weaknesses or concerns in their existing GRC programs. “As it relates to IT, GRC must focus on security. In today’s dynamic and fast-moving business environment, organizations that do not develop and nurture strong GRC practices around IT are more vulnerable to successful cyberattacks,” says Richard Chambers, president and CEO of The Institute of Internal Auditors. “From simple yet brutally effective phishing schemes to more sophisticated cyber hacks, the current IT environment must be viewed as a host for significant risk within all organizations.”

Indeed, David Cullinane, co-founder and adviser of the Cloud Security Alliance and founder of the Global Security Risk Management Assistance group, points out that “businesses make risk decisions all the time...demonstrating security risk in the same terms as the business uses is another major challenge.” In other words, as risk management becomes more tightly intertwined with business, IT security professionals are more than ever under the gun to understand and communicate how managing risk and compliance for cybersecurity objectives fits in with the organization’s over-arching business goals and operations.

A common mistake IT security executives make, Cullinane points out, is confusing their IT security compliance with managing their organization’s risk and security.

“Compliance does not equal good security,” says Cullinane, himself a former chief information security officer for eBay. Though he still hears CISOs say they are compliant with PCI DSS (Payment Card Industry Data Security Standard), or have met ISO 270XX requirements and use the NIST (National Institute of Standards and Technology) Cyber Security Framework, and so believe they are secure. “But compliance is only part of a good security program. The ques-

Our Experts: GRC

Bruce Bonsall, executive faculty, Institute for Applied Network Security
Richard Chambers, president and CEO, The Institute of Internal Auditors
David Cullinane, co-founder and adviser, Cloud Security Alliance; founder, Global Security Risk Management Assistance
Rocco Grillo, head of the cyber-resilience unit, Stroz Friedberg
Christopher McClean, vice president and research director, security and risk team, Forrester Research
Ed Moyle, director of thought leadership and research, ISACA

14% Only 14% of 290 companies surveyed reported they had “Substantially to Fully Integrated” GRC processes and technology across their organizations.

– OCEG
tion a CISO does not want to have to answer is: ‘We gave you all that money for security and we still got breached? What did you do with all that money?’ Telling them ‘I brought us into compliance with all of the above, but it didn’t protect us’ is not a good answer.”

Cullinane also calls out governance as a critical role for the CISO, but one that is seldom understood. Governance includes defining and publishing policies and standards – as well as ensuring that those requirements are being met, he points out. “It’s also one of the reasons I am not a fan of the CISO reporting to IT,” Cullinane says. “If your CIO or CTO will accept you calling out issues and ensure that the issues are resolved, it can work very effectively. But the CIO or CTO has to see that as one of your key functions.”

Governance also means being able to see when significant change is required and being willing to make those changes when it’s security that needs to change, he adds.

The two biggest GRC weaknesses relating to IT security actually are ones that can be most readily addressed and mitigated, according to Chambers. The first is the oft-cited human factor, he says. “From bring-your-own-device [BYOD] challenges to social media-related reputational risks to business email compromise scams [BEC], the vulnerabilities lie in the behavior of employees or members of the organization,” Chambers says.

Similarly, he adds that many organizations focus solely on preventing a cybersecurity breach, with little or no planning for how they will respond when a breach actually occurs. “It is crucial for organizations to have cybersecurity crisis management plans in place that address securing the system after a breach is detected, assuring business continuity, clearly identifying the responsibilities of key stakeholders, and strengthening security efforts post-breach,” he says.

The internal audit function must play an integral role of providing assurance on the effectiveness and efficiency of those efforts, he emphasizes.

Bruce Bonsall, a member of the executive faculty at IANS, the Institute for Applied Network Security, and a former CISO for Mass Mutual, believes that the role of IT security in GRC really varies by industry, the age or maturity of the company itself and the business model. “As organizations evolve, risk is seen more as a business issue,” Bonsall says.

Many smaller organizations might have a more difficult time fielding a good GRC program because managing risk and compliance is seen as too big and too cumbersome, particularly in industries like financial services and health care where compliance is more of a moving target.

Investment firms are one case in point. In January 2016, U.S. financial regulatory agencies began releasing this year’s lists of new compliance issues and concerns – with the Office of Compliance Inspections and Examinations (OCIE) at the U.S. Securities & Exchange Commission (SEC) putting cybersecurity at the top of its examination priorities. OCIE is responsible for conducting examinations of organizations registered under SEC regulations, including broker-dealers, transfer agents, investment advisers and investment companies.

OCIE’s 2016 priorities include advancing the efforts it began the previous September to examine the cybersecurity controls and compliance of broker-dealers and investment advisers, including testing the implementation of the firms’ procedures and controls. Regulatory consultants recommend that advisory and investment firms ramp up their cybersecurity compliance and conduct penetration testing.

Global internet traffic is expected to grow to 1.4 petabytes per second.

– The TABB Group
and mock breaches in order to prepare – with the expectation that increased fines and penalties will be coming down the pipeline.

“Good GRC is largely a matter of how the industry has matured,” Bonsall says.

For example, banks are typically further ahead in recognizing the value of their information systems and protecting against threats, as these institutions have been more under the gun of regulatory compliance for much longer than organizations in other sectors, he says. “Other organizations are just now realizing the value of their information and the many things they need to do to protect it,” Bonsall adds.

While many organizations are embracing a deeper and more business-focused approach to GRC, too many are still looking at managing risk and compliance as a technology problem alone, according to Rocco Grillo, executive managing director and head of the cyber-resilience unit for the legal and technology consultancy Stroz Friedberg.

“There are a lot of great GRC technologies out there, but risk management is not just about implementing technology,” Grillo points out. “It’s more about the tone at the top.”

Organizations are improving in their approach to governance, risk and compliance, but Grillo says that addressing risk management as a C-suite and board-level issue is still a necessary (but often missing) component. Organizations might be addressing risk from a security operations or policy perspective, but the overall organization is not aware of more over-arching business risks, Grillo says.

“If there’s a deficiency that is being overlooked, that will be the one that gets you.”

But, in order to get there, Grillo adds, organizations need to break free from the “check-the-box mentality” regarding compliance and risk.

Christopher McLean, vice president and research director for the security and risk team at Forrester Research, agrees that most large companies are putting more emphasis on risk and compliance and have improved at various aspects of compliance, like Sarbanes-Oxley controls in financial services or remediation process documenting. “But few take a broader look at risk as an organization,” McLean says. “It is unbelievably difficult.”

While companies understand the general needs to manage risk and protect information, McLean says it is more difficult to corral all the necessary stakeholders beyond the security team – heads of sales and marketing and lines of business as well as C-level executives – to determine a more comprehensive, strategic approach to risk controls.

As high-profile breaches like those at Target and Sony capture headlines and compel senior executives and board members to see how lack of compliance and risk controls could affect them personally, visibility for GRC has increased in steps. “It’s a continual march forward,” McLean says.

“When you say GRC today, there’s quite a bit of variety in how people define what that means,” says Ed Moyle, director of thought leadership and research at ISACA (previously known as the Information Systems Audit and Control Association) and a former vice president and information security officer for Merrill Lynch Investment Managers. “GRC has morphed and grown over the years, but not always in a positive way.”

**Threat and response**

That is because GRC is evolving, for good and ill. But many organizations still do not have a broad view of what running afoul of compliance and risk controls can mean to them. And, as with many issues, knowing is half the battle.

“IT security threats themselves have
evolved rapidly,” Bonsall points out. “Phishing, wire fraud transfer scams and social engineering have all exploded from one sector to the next, moving from banking to retail and beyond.” Many organizations are attacked before they realize the scope of the threat, or begin to gear up, he adds.

Case in point: The FBI recently put out an alert on a simple but devastating phishing scheme in the Phoenix area that netted a group of brazen hackers $50,000 on average per incident, according to Chambers. The scheme involved fake emails from CEOs to CFOs or other financial officers directing them to perform immediate wire transfers.

“The apparent widespread success of the scheme suggests poor GRC at those organizations,” Chambers says.

Chambers also recalls a story from a speaker at a recent Institute of Internal Auditors (IIA) conference, who related a tale about one organization’s IT staff automatically sending out proprietary data to a third-party vendor as part of a service contract. The contract ended, but no one informed IT, which continued to diligently send out the information month after month.

“Poor communication and oversight of policies relating to data sharing with third-party vendors led to this breakdown,” he says.

Herein lies a lesson, as McClean points out: GRC is not just about preventing security breaches, but the potential for recalls or for third-party supply chain or vendor incidents.

“One of the biggest concerns in GRC is not knowing where data is or where it is coming from,” Grillo says, referencing the increased use of distributing data storage and management among third-party vendors and cloud computing providers. “When you look at global organizations with complex environments, you may think you have the right controls in place but you can get hamstrung really quickly. All too often companies jump out and try to implement technology without having done an assessment of its impact.”

Moyle believes that the lion’s share of GRC resistance within most organizations comes from “people trying to boil the ocean from day one.” He adds that many companies start out with grand plans to spend in upwards of $10 million to “just redo everything they’re doing already, and add a lot of burdensome processes...It really becomes viewed as antagonistic to business agility and getting work done.”

Instead of biting off more than they can chew, and making enemies in among their business-line colleagues, Moyle suggests that IT security professionals look at what they can accomplish on smaller investments and in less time, even if it only solves 80 or 90 percent of the issues.

“So many business leaders see GRC as expensive and slowing the business down, and that can be true. But it doesn’t have to be,” Moyle says. “GRC can be implemented in lighter-weight ways.”

Cullinane agrees that having a more focused approach is a good way to start the ball rolling. CISOs should not just consider all potential risks, they should prioritize their compliance and risk management goals and ask, “Where are my greatest risks so I can spend my limited budget appropriately to reduce the risk of bad things happening?” he says. “You must use risk management to protect against the bad things that are most likely to happen.”

But how does employing this kind of priority-setting in GRC look in practice? Cullinane offers an example: Patching vulnerabilities is key to good security, but in a large, complex environment with thousands of servers, network devices and applications, “keeping them all patched is an almost impossible job...
and is extremely labor intensive for IT under the best of conditions,” he says.

“Governance means recognizing the issue and finding ways to reduce the workload, while improving security, not just auditing for compliance,” he continues. So, instead of trying to play the impossible Whac-A-Mole game of patching all vulnerabilities all the time, an organization should use a vulnerability assessment vendor to help identify those vulnerabilities that could be most easily exploited in their environment, or be most detrimental, as opposed to a long laundry list, he adds.

Moyle points out that many organizations still do not take full advantage of the frameworks and guidelines put out by general standards bodies, such as NIST or industry-specific groups. “It’s not always about cybersecurity, but risk management activities,” Moyle says. “They codify a lot of good practices that could enable an organization to do GRC well…and more people should at least look at it, to either use it or consider customizing it to their environment. Why not use the work of other folks, rather than try building GRC from the ground up?”

Problems often emerge, Moyle says, when organizations jump the gun and buy expensive or ill-fitting GRC technologies or tools without first assessing their needs for risk management and compliance or setting priorities. He also recommends that IT security professionals consult with internal auditors more actively, since “they know more about the internal workings of the business than anyone else.”

Cullinane agrees about IT security and audit working more closely together. “People are less hard to find than technical people,” Cullinane says. He usually asks one of the audit managers to come over to the dark side and help on GRC programs. “It works very well because they know where the issues are that need to be addressed – and they have been trained in the concepts.”

Technology still plays an important role. As risk and compliance become more complex, automation is becoming a more necessary part of the equation, industry experts admit. While most organizations still rely on more traditional methods, the more modern automated monitoring and control systems can be more effective in identifying weaknesses in GRC controls, according to the “2016 OCEG GRC Tech Strategy Survey.” (OCEG, a GRC think tank, originally was known as the Open Compliance and Ethics Group, but now just uses the acronym.) The survey found that fewer than 20 percent of respondents build GRC controls through IT when it comes to automated control enforcement, compliance management, internal controls, business continuity, IT GRC management, risk management analysis and third-party management. However, the survey also found that spending on IT in those areas will increase on average by 51 percent over the next three years.

“GRC programs are only as good as the technologies and strategies used to build them and the people who end up executing those strategies,” Chambers says. “Organizations should constantly be reviewing the effectiveness and efficiency of GRC-related policies and practices. Establishing policies to mitigate risks, communicating those policies effectively and testing for compliance will help reduce those risks.”

**Risk and reward?**

As massive an undertaking as GRC can be, it is little surprise that there are still a number of obstacles to implementing an effective risk management and compliance program that stays in step with the changing needs of an organization. According to McClean, the greatest challenges are almost always organizational.

“There are great technologies and terrific
best practices out there, but the challenge is almost always internal,” McClean says. “There’s always disagreement about how much to invest, or getting customer-facing colleagues to understand risk assessment.”

Chambers points out the hurdles that many companies are facing: insufficient resources, rapidly changing technology, regulatory pressures and a dynamic business environment where new and emerging risks can develop overnight and all pose challenges to good GRC.

The key to moving forward, Chambers says, is for “organizations to develop strong and effective systems where risk management responsibilities are clearly understood.”

To that end, the IIA promotes the use of the “three lines of defense model” to spell out clearly the roles of management, audit committees and boards, as well as internal audit to identify and mitigate risks and to provide assurances of the effectiveness of those efforts.

Additional outside influences from external auditors, regulators and investors provide additional levels of complexity, Chambers adds.

But there is often an even bigger issue afoot, according to Moyle. “One large obstacle is the perception that GRC, as an activity, is just not useful,” Moyle says. “I think it is useful and necessary, and there’s a perception gap…and a lot of budgetary concerns.”

The crux of this issue is sometimes that while IT security and risk management are intrinsically linked, “security is not purely a technology issue...[and] many CISOs grew up as technical people and have no experience or training in risk management,” Cullinane says. “The CISO’s job is risk management. Governance and compliance are critical components of risk management.”

Case in point: While Cullinane was the CISO at eBay, the CFO told him that he could give $100,000 to a business unit and they would make him $1 million in revenue. “He asked me, ‘What was I going to do for him?’ I had to be able to show him that I was going to reduce risk by X dollars.” Cullinane says. “That is where most security programs and leaders fail. They don’t know how to do that effectively.”

Hence, Cullinane also points out that while quantifying risk in dollar terms is difficult, CISOs need to consider how to demonstrate in business terms the current threat level to their business and how much a security control or compliance control will reduce that risk. “If fraud is a problem for your company, you can demonstrate that in terms of dollars of fraud reduction,” he says. “If you can’t use fraud, the problem becomes far more complex.”

According to Chambers, good GRC management is “at the heart of all successful organizations.” Since today’s business strategies are risk-based, each organization must have a strong understanding of the risks it faces, its risk tolerance, key risk indicators that can alert them to changing business conditions, and a way to assess how it is managing and mitigating risk.

“When risks are clearly identified and well-managed, organizations are well-positioned for financial success, competitive advantage, successful expansion, return on investment and boosting the organization’s overall value,” Chambers says.

For more information about ebooks from SC Magazine, 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.
RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA’s award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime. In today’s competitive landscape, risks are dramatically changing and with increasing complexity, next generation security strategies are critical.

RSA Archer provides GRC professionals with a centralized solution to identify, assess, evaluate, treat, and monitor risks across the lines of business. Areas of focus include IT security and risk management, operational risk, regulatory and corporate compliance, audit management, business resiliency, and third-party governance.

For more information, visit www.rsa.com
Harness Risk, Fuel the Enterprise
RSA Archer