Storing the personal data of just one EU customer means the GDPR’s stringent new rules can result in huge fines, and maybe even criminal charges.

The board of directors must take a leadership position in moving an organization into compliance with the European Union’s impending General Data Protection Regulation (GDPR), which takes effect in May 2018. Rather than taking a passive approach and relying on others to understand the issues and resolve them, the board must become more involved – but this doesn’t mean the board has to take a cybersecurity crash course. Rather, as GDPR can impact any enterprise, including smaller businesses and nonprofits, with breaches potentially resulting in substantial penalties, boards should start by asking questions about their organization’s level of readiness for GDPR, and consider allocating resources to ensure the company is compliant by the May 25, 2018, deadline.

GDPR REPRESENTS THE MOST STRINGENT REGULATION ON DATA PRIVACY TO-DATE – WITH GLOBAL REACH

It seems every week there is yet another data breach that impacts millions of individuals and results in personal information being disclosed. Governments have taken notice, and as many companies have proven to have questionable reliability at protecting an individual’s privacy, governments are starting to step in with new regulations and statutes. Perhaps the most well-known, far-reaching and impactful of these new legislative initiatives is the European
Union’s General Data Protection Regulation (GDPR). The new rules require the company’s directors and officers to certify that their company is in compliance – and holds them personally accountable. Here are four questions directors and officers can discuss to ensure they are up-to-speed with GDPR.

**Q1. HOW MUCH IMPACT WILL GDPR HAVE ON THE BOARD AND DIRECTORS?**

In contrast to other relatively vague and toothless measures, GDPR is very specific, with identifiable requirements and penalties that can result in huge fines, as well as personal criminal liability for board members. GDPR is not just an EU-specific regulation – every EU citizen’s private data, regardless of where it is stored, must be protected. In today’s world of Web-connected businesses, even small organizations not located in the EU may have customers from EU countries and are, therefore, subject to aspects of GDPR.

The regulation requires that businesses take concrete steps that include the following:

- **Designation of a data protection officer** in any organization where there is “regular and systematic monitoring of data on subjects on a large scale or where the entity conducts large-scale processing of special categories of personal data.”

- **Data protection, including the use of encryption.** GDPR provides specific suggestions, including “pseudonymization” or encryption of personal data, the ability to ensure ongoing confidentiality, and a process for regularly testing to ensure protection.

- **Explicit consent by customers to store or use their data.** Despite an organization having access to email addresses, the customer retains ownership. Additionally, permission can no longer be implied and the default can no longer be to give the company permission. Customers must actually check a box or use a similar method to actively grant permission for a company to use their email address. Customers also have the right to receive a full accounting of everywhere their data is stored, how it is used, and may request all of their data to be purged at any time.

Among the most important differences between GDPR and previous regulations is that for the first time, the organization’s board of directors is held accountable for protecting data. Board members must now become active participants in certifying data protection and be the drivers of internal processes and actions to protect customers’ private information. Additionally, directors themselves will have to be conscious of how, when and where they store any board-related documents or communications that contain EU citizen data.

The penalties for failure are groundbreaking, with fines as much as 4% of annual worldwide turnover, or €20 million, whichever is higher. Meanwhile, GDPR reinforces the potential for criminal prosecution to be sought against directors and officers for deliberate breaches. Simply put, board members could go to jail.

In much the same way that the Y2K issue drove a fundamental assessment of an organization’s systems and processes, so too will GDPR. Make no mistake; this will be a sea change in how companies do business and how they protect personal information. There will be an impact in most operating groups, notably IT, marketing, customer service, sales, risk management and, most of all, the executive suite.

Furthermore, there is still plenty of work to be done. A recent Compuware study shows there is still a long way to go. Only 60% of U.S. companies have plans in place to respond to the demands of GDPR, while 94% possess customer data for citizens of the EU. Getting to compliance won’t be easy: 85% of the survey respondents say it’s difficult to know exactly where data resides, which is a key component of GDPR.

**Q2. IS THE BOARD SETTING THE TONE FOR CYBERSECURITY?**

For the first time, GDPR focuses the cybersecurity issue personally and directly on board members. Outside directors are also included and there is almost no way to deflect this focus to absolve board members of responsibility. GDPR leadership has to start from the top: the board must move from being merely “observers” to being the leaders of cybersecurity practices.

This will demand modification of current thinking. The status quo for most board members is to act as “consumers” of metrics and information provided by the operating teams regarding cybersecurity solutions, and then accept those teams’ assessments of the level of protection. GDPR requires that the board become active drivers of better data protection processes.

Recent surveys showcase the current thinking and the need to change. According to the Spencer Stuart “What Directors Think” survey, 38% of directors think that cybersecurity risk is “out of their hands.” This is troubling, but this same survey shows an implicit understanding of the need for increasing expertise,
as 83% of directors think that it is at least somewhat important to consider IT/Cyber expertise as a key skill for new directors.

GDPR is not the only new set of regulations demanding that directors become not only more active, but also more knowledgeable in the future. The U.S. Cybersecurity Disclosure Act of 2017 (S.536) includes a requirement to disclose what cybersecurity expertise exists on the board. If that expertise is lacking, the company must list what cybersecurity actions have been taken by the organization in place of board direction. Further, in the case of a breach, the company will be held responsible if directors’ lack of awareness and cyber-readiness slows down breach notification. It should be noted that the current iteration of the Cybersecurity Disclosure Act is the second version, supplanting the bill filed in 2015. It is quite possible that the final version of this bill may include some elements of GDPR.

Q3. HOW “CYBER-SAVVY” IS THE BOARD? – TIME TO MAKE EVERY DIRECTOR “CYBER-SMART.”

To take on the leadership role, board members must have real cybersecurity knowledge and a reasonable level of expertise. Cyber-ecurity expertise has not been a core strength sought out in candidates for most director positions. The vast majority of directors are coming in with finance, legal and business backgrounds. A recent article in SC Media reported that only 5% of companies on the Financial Times Stock Exchange (FTSE) have cybersecurity expertise on the board. In addition, Accenture has found that only 6% of the directors at the world’s largest financial institutions have technology expertise. The data in North America is hardly better, with only 12% of directors having a professional technology background, according to the same Accenture report. Clearly, the board is going to have to build or acquire new cybersecurity skills going forward.

Unfortunately, most boards have a long way to go to reach the goal of being cyber-savvy. A recent article in the Harvard Law School Forum on Corporate Governance and Financial Regulation strongly suggested that the board itself create a board committee focused on cyber risk and cybersecurity that covers the gamut of potential threats from both internal and external parties, including strong data protection capabilities. The article makes it clear that directors need to deal in specifics, rather than an “overview” approach.

Q4. DO THE BOARD AND ITS MEMBERS PRACTICE GOOD CYBERSECURITY HYGIENE?

Directors need to focus on the cybersecurity issues that impact their organization and a good starting point is to look at their own cybersecurity practices. Directors that take a lackadasical approach to cybersecurity in their personal interactions with the company will find it difficult to be leaders on this initiative. Personal experience and interaction with policies and systems that deliver cybersecurity provide an important perspective for directors.

One startling fact that jumps out from a recent survey done by the NYSE and Diligent shows that 92% of directors use personal and unsecure email for communications with management and other directors. Worse, 54% have downloaded board books or company documents onto their personal devices. Directors change their perception that the combination of their lofty position and “outsider” status exempts them from standard corporate cybersecurity policies. The Diligent Boards and Messenger products can solve this problem quickly and provide directors with the truly secure experience from which they can learn.

There needs to be a sense of ownership for cybersecurity issues as core to business success. This starts with a more active posture in setting the tone for effective cybersecurity that starts with directors changing their own lax processes.
**Diligent Solutions Support the “Cyber-Aware” Board and Directors**

Diligent, a leader in solutions for boards and directors, provides many products that help increase the directors’ cybersecurity posture by reinforcing best practices around mitigating cyber risk. Diligent’s secure communication and collaboration solutions bring a security-centric process to the workings of the board.

**Diligent Boards**

Diligent Boards is a secure portal for all board agendas, documents, annotations, discussions and board books, reducing the risk of having confidential information compromised on a personal device. This solution encrypts data to ensure that all sensitive board materials are protected.

**Diligent Messenger**

One of the weakest links in cybersecurity is public and even corporate email systems. Diligent Messenger is a confidential and secure communications environment for board interaction that goes well beyond traditional email systems. Messenger also provides a secure repository for data, eliminating the need for directors to store their own, possibly unsecured, copy.

**Diligent Evaluations**

Board evaluations are often done randomly or without a process to drive meaningful results, blocking change. Using Diligent Evaluations, it is now possible to have real data on the board’s level of cybersecurity expertise, critical information in light of the Cyber-Security Disclosure Act. Diligent Evaluations will help keep directors and committees on track, compliant and continually focused on improving board performance.

This product simplifies the information-gathering process to document board members’ knowledge, experience and expertise. The confidential, online process simplifies what is often a complex and high-cost project that requires far too much human interaction.

---

**Summary**

New regulations and statutes such as GDPR are mandating that boards and individual directors become focused and engaged on cybersecurity issues. Perhaps what is most important for the individual director is that they may be personally responsible for cybersecurity-related issues. As the number and breadth of massive data breaches increase, voters will demand new statutes and regulations with a focus on making corporate management and boards responsible parties for protecting personal information.

GDPR will provide an important “test case” that other countries and jurisdictions will watch closely. It is unlikely that the focus on holding individual directors responsible for cybersecurity will abate. Data breaches have only raised the general level of distrust of “big business” and a corresponding increase in the desire to hold the top executives responsible. Board members must increase their cybersecurity skills, engagement and awareness. An excellent place to start the change process and to personally learn more about cybersecurity is to ensure their interactions as board members are done in a highly secure and well-protected environment.

5. https://corpgov.law.harvard.edu/2017/01/12/a-strategic-cyber-roadmap-for-the-board/