Directors Need to Set the Standards and Expectations for Management to Establish Well-Staffed and Well-Funded Cyber-Risk Framework

Much like any response plan, a cybersecurity framework is only successful if it is well-staffed and well-funded. Otherwise, it simply will not be able to adequately handle the stresses caused by a breach. In a world where malware and ransomware are increasing both in frequency and severity – Wannacry, for example, affected 200,000 computers in 150 countries – to be anything less than well-prepared is a mistake that will almost certainly result in a company's systems being compromised severely.

Unfortunately, just because companies should have cybersecurity teams that are well staffed and funded doesn't mean that they do. In fact, the opposite is more likely to be the case. Companies have often been slow to catch up to the admittedly rapidly changing cyber environment. Instead of having systems that are well-integrated between departments, reporting structures and decision-making systems are very segmented, often by department, resulting in mess of systems that are independent of each other when they should be interconnected. This is largely the result of being too slow to adapt to the changing nature of cybersecurity and is a legacy problem of companies. After all, a disjointed and disconnected system in a company is not going to be able to effectively prepare for or react to an exploitation of the very connected nature of modern technological systems.

To rectify this very disjointed mess of systems, a company first must assess how sufficient their systems already are. Luckily, there exists a system in place to do just that. Thanks to President Obama's Executive Order 13636, the National Institute of Standards and Technology (NIST) was instructed to create a cybersecurity framework that could be adopted in a voluntary manner by the private sector, with such a framework being released in 2014. In the NIST Cybersecurity Framework, companies are able, and encouraged, to review their risk-management process in such a way that it place them in one of four different tiers:

- Partial, the lowest tier,
- Risk informed,
- Repeatable,
- Adaptive, the highest tier.

By using this baseline evaluation, companies will be able to determine what level of preparedness they currently have and can then build off of that to improve their cybersecurity readiness. And due to the NIST Framework's voluntary nature, the uniqueness of companies will not be an impediment as a company can evaluate whether it is capable of such management.

Once the Board of Directors has conducted this evaluation of their systems, they might be thinking, "Ok but what now?" After all, realizing what tier of readiness the company sits at doesn't mean the problem is dealt with. Thankfully, there exists an answer to this question. In the recently revised Cyber-Risk Oversight Handbook, which NACD published in collaboration with ISA and AIG, there is a series of seven recommendations on how to develop a more integrated approach to cyber risk. These recommendations address both the need for the company's cyber

team to be interconnected throughout the company and have the financial resources to do their job effectively. These recommendations are:

1. **Establish ownership of cyber risk on a cross-departmental basis.** The Board of Directors should place a manager with cross-departmental authority as head of the team so as to ensure the team is led by someone who is already integrated in multiple sections of the company.
2. **Appoint a cross-organization cyber-risk management team.** As common-sense as it seems, the only way to have a cyber team that is interconnected is to have members of the team be from each department of the company, not just the IT department.
3. **The cyber-risk team needs to perform a forward-looking, enterprise-wide risk assessment.** Much like the last recommendation, this just makes sense. You can't be adequately prepared if you're not looking ahead, and a cyber-risk team won't be effective if it is not assessing the enterprise in its entirety. Special attention should be paid to regulatory compliance
4. **Be aware that cybersecurity regulation differs significantly across jurisdictions.** This is very important, as depending on the size of the company, the cyber team may have a jurisdiction as small as one state or as large as multi-national. Management should make sure they are fully in compliance with these jurisdictions, and the Directors must ensure management has the resources to do so.
5. **Take a collaborative approach to developing reports to the board.** Collaboration is key. The only way to effectively tackle enterprise-wide cybersecurity is through interconnectedness between the management team and the Directors. Executives should ensure evaluation of cyber-resiliency is conducted quarterly.
6. **Develop and adopt an organization-wide cyber-risk management plan and internal communications strategy across all departments and business units.** While cybersecurity might seem like an IT issue on the surface, it is not and must be organization-wide if it is to be successful. Every department must feel part of the team and should have a role in developing the corporate plan.
7. **Develop and adopt a total cyber-risk budget with sufficient resources to meet the organization's needs and risk appetite.** This is both tricky and very important. Due to the cybersecurity talent gap, resource evaluation on the part of the Directors is integral to determine what can be done in-house and what must be shopped out to third parties. Most important, cybersecurity is not just an IT issue and therefore the budget must be more than just an IT budget. Resources must be allocated from each department otherwise it will not be adequately prepared.

By following these recommendations, the Directors of the company will be able to set standards for management to have a well-funded and well-staffed cyber-risk team. This is paramount because if this team is not comprised in a cross-departmental fashion, and without proper resource support, the Directors are leaving themselves needlessly open to risk and could be perpetuating the mistaken belief that cybersecurity is just an IT issue.

Written by Larry Clinton, ISA President & CEO, and Nicholas Dowse, ISA Manager of Office Operations and Communications