A CALL TO ACTION: CYBERSECURITY DUE DILIGENCE IN TODAY’S BUSINESS CLIMATE

Steven Grimberg∗
Mark Ray∗

These days it is the rare news cycle that goes by without referencing the latest cyber-related data breach to impact some fill-in-the-blank, well-known consumer-based company. Long gone are the days where executives and Board members did not worry about cybersecurity for their respective organizations, but incredibly too many of them continue to admire the problem or pretend that “it won’t happen to us” until, well, it does.

So, what can be done about it? The answer, consistent with traditional views of corporate governance best practices, is to engage in due diligence—proactive action by asking the right questions to the appropriate personnel both internally within the company, as well as externally. The common denominators of good cybersecurity preparedness, regardless of size, scope, or industry, are front-end assessments, planning, and testing.

Cybersecurity Assessments

Managing today’s cyber risks starts with identifying and addressing the vulnerabilities and gaps in the organization’s information security program. This can be accomplished by analyzing the security program against one or more of the major pillars of globally accepted guidelines, such as the NIST (National Institute of Standards and Technology) Cybersecurity Framework1, or the UK National Cyber Security Centre’s (NCSC’s) Cybersecurity Guidelines2 Well-performed assessments evaluate the people, processes, and tools that comprise the security program to not only identify areas of

∗ Steven Grimberg is a former federal prosecutor with the U.S. Department of Justice who led a cybercrime unit and investigated complex and high-profile criminal and national security-related cyber incidents. He is now General Counsel and a Managing Director for Nardello & Co., a global investigations firm, that specializes in cybersecurity planning, incident response and crisis management. Mr. Grimberg is also an adjunct professor at Emory Law School.

∗ Mark Ray is a former special agent with the Federal Bureau of Investigation who led global investigations involving transnational cyber-criminal organizations. He is a Managing Director and Head of the Digital Investigations & Cyber Defense practice at Nardello & Co.


improvement to protect information and data in the first instance, but also to reduce the impact of the inevitable cyber-related incidents.

A cybersecurity assessment should begin with information and data collection. The assessment team should conduct thorough interviews of internal and external IT service providers and other key stakeholders to obtain a baseline understanding of the organization’s current cybersecurity program. The collected information and data should then be analyzed against a cybersecurity framework such as NIST and, if applicable, industry-specific compliance guidelines like the US’s Health Insurance Portability and Accountability Act (HIPAA). The assessment should culminate in the preparation of a report for key organizational stakeholders that consists of investigative findings, rankings, and a prioritized list of actionable recommendations. However, the key to a successful assessment report is the word “actionable”. No organization will ever achieve perfect security, so providing them with a list of recommendations that cannot be reasonably implemented (from a cost or time perspective) does them no good. Organizations need to be provided with a list of actions that they can reasonably achieve based on their threat and risk profile.

The benefits of pro-active, front-end cybersecurity assessments are straightforward and multi-fold. They illuminate security and compliance gaps and reduce both the likelihood and impact of data security incidents. They prioritize cybersecurity budgets and resources. Also, they could help keep regulators at bay, both before and after a cyber incident, by demonstrating good cyber hygiene and best practices.

Incident Response Plans

Another critically important component of cybersecurity due diligence is preparing and maintaining an effective incident response plan. Generally, an incident response plan sets forth the internal organizational guidelines for responding to a cyber-related incident, identifying particular assignments or duties for identified personnel, and establishing a communications protocol if the network has been compromised.

Most organizations have some semblance of an incident response plan in place, but too many of them have a one-size-fits-all approach embedded in their plans that are geared towards responding to a major cyber incident or massive data breach. The reality is that most organizations, regardless of size or scope, have cyber-related incidents every day. These incidents come not just from external sources, but insiders as well (i.e., the lost or stolen organization
laptop or phone incidents). The modern-day incident response plan should reflect modern-day issues that arise and be more granular in approach.

To accomplish this, organizations should prepare an incident response plan that utilizes a clearly defined severity matrix. The severity matrix distinguishes response protocols based on the type of incident as well as the number of systems and data sets potentially impacted. This helps define the level of escalation required, both internally and externally, based on the scale of the incident. For example, depending on the size and scope of the organization, a “level one” incident may not need to go beyond IT/Security personnel, whereas a “level three” incident may require immediate notification to one or more executives, engagement with inside and/or outside legal counsel, as well as include a public relations component. The key is to customize an organization’s incident response plan based on the import of various data sets that could be compromised.3

Lastly, many incident response plans omit or do not clearly define how communications will occur with outside entities. In many data breach incidents, managing communications and coordination with outside entities (i.e. law enforcement, regulators, media) becomes as burdensome as containing the technical aspects of the breach. Pre-establishing relationships with these entities, and clearly defining the chain of communication with them in incident response plans, can greatly reduce the impact of an incident.

Testing Incident Response Plans

The final step towards diligent cybersecurity preparedness is testing your organization’s level of preparedness for responding to a cyber-related incident. Too many times, organizations that believe they have done a good job of preparing for a cyber incident unfortunately realize, in the middle of an actual event, that the organization has become overly dependent on particular personnel and institutional knowledge that is stored only in their heads or on a set of factual assumptions that simply do not square with the reality of incidents that are inherently unpredictable and multi-varied in scope and size.

One of the best, most cost-effective methods for organizations to test their incident response plans are through so-called tabletop exercises. Tabletop exercises are analogous to a fire drill, where a hypothetical cyber incident scenario is developed and played out, ideally involving not only those

---

organization personnel with direct responsibilities under the cyber incident response plan, but also executives who have decision-making authority when it comes to budget resources and prioritization. Like the incident response plan itself, the tabletop exercise should be specifically tailored to the organization that is utilizing it and not be just an off-the-shelf product.4

CONCLUSION

Cyber-related risks are a reality that all organizations face regardless of industry, size or scope. Following good front-end cybersecurity hygiene, such as the steps outlined here, can help minimize the frequency and impact of incidents when they do occur. And they will.

---