CYBERSECURITY

PREPARING FOR A DIGITAL ARMAGEDDON

By Kelly L. Frey, Sr.

We are under attack. Whether it is cyber-theft, cyber-terrorism, or cyber-warfare, critical systems that generate and distribute electricity on the grid, control commercial aircraft in flight, process bank and credit card transactions, coordinate our traffic lights, authorize military action, and control emergency response are targets of daily assaults by hackers whose goal is to penetrate, disrupt, and/or exercise control over critical infra-structure in the United States. It is a battle we are losing.

Headlines have recently concentrated on cyber-security incidents that affect the consumer. Identify theft from cyber-security breaches now cost the victim over $500 and 30 hours of remediation work per incident. But the hacking one person is nothing compared to hacking into data systems that house information on millions of consumers. Most recently, financial data from millions of Target customers was stolen by hackers who targeted credit card (Point of Sale or POS) terminals in its stores (a massive data breach that compromised 40 million credit/debit card accounts between Nov. 27 and Dec. 15, 2013). As of the date of this article, Target's cyber-security breach has resulted in $17 million of net expenses (although total expenses were $61M, such losses were partially offset by $44 million in cyber-security insurance payments). The loss resulted in almost a 50% reduction in 2013 fourth-quarter profit for Target (and a 5.3% reduction in total revenue as the breach scared off customers).

And commercial systems are not the only digital assets we need to worry about. FBI director James Comey told the Senate homeland security and government affairs committee in September 2013 that cyber-attacks were likely to eclipse terrorism as a domestic danger over the next decade. "That's where the bad guys will go," Comey said. "There are no safe neighborhoods. All of us are neighbors [online]." In fact, a 2013 report by the Secretary of Defense noted that "In 2013, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military".

We must now protect ourselves not only from the bored teenage hacker – we now have to worry about how to defend ourselves against organized international crime syndicates paying millions of dollars to expert information technology (IT) professionals and foreign governments tapping the best and brightest professional IT talent within their jurisdictions for nationalist purposes.

Protecting Critical National Infra-structure

Lacking a clear legislative process with respect to cyber-defense, the executive branch has stepped in to create an over-arching framework to assess current vulnerabilities of companies involved in owning or operating critical infra-structure and to effectively deal with inevitable cyber-security breaches.

A Framework for Improving Critical Infrastructure Cybersecurity (the "Framework") was developed by the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) in response to an executive order by the President of the United States to assist (a) owners and (b) operators in 18 critical infrastructure industries (ranging from energy to transportation and communications) in preparing for, preventing, mitigating, and responding to cybersecurity threats. The Framework draws heavily on existing technical standards (such as NIST 800-53 Rev 4, ISO 27001:2013, ISA 62443-2-1:2009, and COBIT 5) and addresses management of cybersecurity risks "for those processes, information, and systems directly involved in the delivery of critical infrastructure services".

The Framework Core (Core) is a set of cybersecurity activities, desired outcomes, and applicable references that are common across all critical infra-structure sectors and business. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes within an organization and across organizations/with the government. The Core defines 5 cybersecurity "Functions" that provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risks. The Identify function mandates that an organization develop an enterprise-wide understanding of risks to systems, assets, data, and capabilities. The Protect function mandates that organizations develop and implement safeguards to assure continuous operation and delivery of critical infra-structure services during and after a cyber-intrusion. The Detect function mandates that organizations develop and implement activities to timely identify, communicate, and escalate cyber-security threats within the organization and with critical private/public partners. The Respond function mandates that organizations develop and implement appropriate activities to take regarding any detected cybersecurity event or intrusion. The Recover function mandates that an organization develop and implement activities to maintain resilience and to restore any capabilities and services that are degraded as a result of the inevitable unauthorized intrusion.

Within each Function, the Core defines Categories (such as Asset Management, Access Control, and Detection Processes) and subcategories (for specific outcomes of technical and/or management activities) with appropriate annotations to Information References (standards, guidelines, policies, and practices). Using the Core an organization can map its assets and vulnerabilities, as well as its response and remediation plans and provide a resource guide to help inform everyone within the enterprise of the scale of attack and the remediation being done.

The Framework also defines Implementation Tiers to classify organizations based upon their cyber-security readiness. The Tiers range from Partial (Tier 1 - where risk management practices are not formalized, there is limited awareness within the organization with respect to threats/responses, there are only ad hoc response systems and protocols, and there is no coordination outside of the organization) to Adaptive (Tier 4 - where continuous process improvements are integrated in an organization-wide manner with clearly defined channels of communication to critical infra-structure partners and governmental authorities). The clear intent is that organizations owning or operating critical infra-structure capabilities will progress over time from Tier 1 to Tier 4 status.

With respect to implementation, the Framework provides directions with respect to organizations creating a "Profile". The Profile is designed to map the Functions to current organizational capabilities. The result should be essentially a gap analysis that outlines deficiencies with respect to cyber-preparedness. The organization would use this gap analysis to develop a strategy to remediate cyber-security deficiencies and improve responsiveness to cyber-intrusions.

Legal and Governance Implications of the Framework

Beyond the technological aspects, perhaps the most significant, and underappreciated, aspect of the Framework relates to the new oversight responsibilities with respect to cyber-security required from the Executive Level within an organization. The Framework makes it clear that cybersecurity is not just a technical problem to be addressed by information technology specialists. Instead, the Framework articulates cybersecurity as a core responsibility of the Executive Level (a defined term within the Framework).

This emphasis is consistent with the increasing focus on cybersecurity by board members and C-suite executives of US companies. In the Framework, the Executive Level is charged with communicating mission priorities, making appropriate resources available, and developing an overall risk tolerance within the organization as part of an integrated cybersecurity program. The Executive Level is also charged with monitoring outcomes. The implication is that board members and C-suite executives must exercise reasonable care and due diligence with respect to the cybersecurity of their companies as an integral part of their fiduciary duties (and may be charged with a breach of this fiduciary duty if they fail to be adequately informed or take commercially reasonable actions to remediate cyber-security issues). Such mandate would seem to anticipate a higher level of civil and potential shareholder liability at the board and C-suite level for cybersecurity breaches than currently exists under US law.

There may also be international implications with respect to the Framework. While designed to address US cyber-vulnerabilities, the Framework is clear that it is not country specific and was developed to create "a common language for international cooperation on infrastructure cybersecurity". This may be especially important for multi-nationals that either own or operate "critical infra-structure" within the US and create extra-territorial mandates for companies with facilities outside of the US that may be portals of entry for US cyber-intrusions. The Framework may also help inform the proposed Directive on Network and Information Security (the Directive) and Cybersecurity Strategy of the European Union, providing a technical framework and lexicon for articulating, and confirming compliance with, such Directive and Strategy. But there also appear to be substantial differences between the Framework and the Directive/Strategy that will need to be rationalized, particularly with respect to privacy and civil liberties. The Framework does not contain controls for protecting privacy or civil liberties, instead noting that "not all activities in a cybersecurity program may give rise to [privacy and civil liberties] considerations". Such approach seems to create an inconsistency between the expansive (and mandatory) data-sharing arrangements anticipated under the Framework and the data protection schemas preferred under the EU Directive/Strategy. This disjunction is particularly troubling given the current state of Data Protection and Safe Harbor discussions between the US and the EU (especially where the Framework creates data sharing arrangements that are specifically prohibited in the EU).

On a national level, it is not clear whether the Framework will be generally adopted outside of the designated critical infrastructure industries. There is currently no governmental regulation mandating adoption even within even the critical industries for which the Framework was designed. Instead, the DHS has merely created a Critical Infrastructure Cyber Community (C3) Voluntary Program to offer technical assistance to organizations that want to implement the Framework. However, the Framework does seem to articulate "best practices" and may create an "industry standard" for all companies in the US against which cybersecurity failures may be judged in civil/commercial litigation. In this regard the "best practice" and "commercially reasonable" threshold set out in the Framework may represent a new basis for shareholder derivative suits against companies and C-level executives that fail to take steps as articulated in the Framework.

Summary and Conclusion

The Framework is clearly required reading for the nerds and geeks within an organization that deal with IT infra-structure on a daily basis. But indications are that the Framework must be reviewed at the highest level of a company, including at the board of director and C-suite level. Board members and C-level executives (who are legally charged with the fiduciary duty of due diligence and inquiry) cannot just assume that their IT professionals will be adequately dealing with the risks presented by digital intrusions. While board members and C-level executives can reasonably rely upon experts in this area to assist them, the Framework makes it clear that the strategy for protecting against cyber-intrusions (and the requirement to apply appropriate corporate resources against such cyber-intrusions) must come from the top of the enterprise. That being the case, it will be incumbent upon board members and C-level executives (and the lawyers and IT professionals providing board and C-level advice) to consider a process for adequately (and regularly) addressing cyber-security during board meetings and C-level executive briefings, especially with reference to the new Framework.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of cybersecurity law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Kelly L. Frey is a Member in Dickinson Wright's Nashville office. He can be reached at 615.620.1730 or kfrey@dickinsonwright.com

This article was first published in the March, 2014 issue of the Nashville Bar Journal, Vol 14, No. 2, page 10 and is reproduced in its entirety by permission.