DEVORE & DEMARCO LLP
ATTORNEYS AND COUNSELORS AT LAW

CLIENT ALERT:
SONY v. Democratic People's Republic of Korea?

To Our Clients and Friends:

As relentless news reports have made clear, Sony Pictures Entertainment has suffered -- and continues to suffer -- a devastating cyber-attack on its computer systems. According to press reports, a hacker group known as the "Guardians of Peace," or "GOP," has taken credit for the attack, which has paralyzed Sony's network and leaked much as 100 *terabytes* of confidential information. Leaked data has included Social Security Numbers, employee and talent salaries, account and administrative passwords, sales plans, sensitive employee emails *and* four unreleased major motion picture films. According to press reports, the GOP used a series of compromised computers in Thailand, Poland, and Italy to launch the malicious software into Sony's network. Once inside, the malware used Windows enterprise tools to (1) infect the computers across the entire corporate network, (2) copy files and data, and (3) then wipe the hard drives of the infected systems.

The attack has prompted an ongoing criminal investigation, and the FBI has issued warnings to U.S. businesses concerning the malware used in the attack. Authorities found the malware's wiping features similar to that used by the Democratic People's Republic of Korea (DPRK) in prior state-sponsored cyber-attacks on South Korean television networks and banks. Unconfirmed media reports also suggest a possible link to the DPRK, which previously threatened to take action in response to a forthcoming Sony Pictures film called *The Interview*, which features a fictionalized CIA-backed assassination of North Korean leader Kim Jong-Un. The DPRK has called the film an "act of war," though it has publicly denied responsibility for the Sony attack. The GOP, however, continue to leak Sony's proprietary information, while demanding that Sony "[s]top immediately showing the movie of terrorism which can break the regional peace and cause the War!" Theaters have cancelled showings, SONY has deferred indefinitely the theatrical release of the film, and a class action lawsuit by SONY employees has been filed against the Company, alleging that it failed to properly protect employee data.

Unfortunately, the fallout of Sony attack presents a growing reality for U.S. corporations facing ever-evolving challenges in information privacy and cybersecurity. The disclosure of confidential corporate information and employee data, whether an inadvertent email or an enterprise-wide breach, present numerous legal and regulatory concerns for businesses. The Sony incident can serve, however, as a useful reminder of several key points:

- First, it is important to recognize that, if and when a technologically sophisticated nation state decides to hack your systems, only military grade defenses stand a chance of

preventing that attack. Simply put, if a nation state is determined to get your data, they most likely can. This does *not*, however, mean that prevention is pointless. Importantly, a well-publicized incident such as the Sony attack can spawn "copycat attacks" by less-sophisticated attackers. Good technical *and* policy controls can defend against these. Now is a good time to review those controls and your overall legal, policy, and technical cyber-resilience.

- Second, given the SONY example, now is also a good time to "road test" your Cyber-Incident-Response Plan. Presumably you have this non-technical, *management-focused* document. If you do not, now is a good time to draft a plan which complies with legal requirements and best-practices standards in this area.

- Third, you should strongly consider conducting a live-fire, tabletop exercise with management to simulate how you would handle a similar event. (Of course, for obvious reasons, this exercise should be done under privilege).

- Fourth, you should take this opportunity to review your data access management, password hygiene, and retention policies. Ask those responsible questions such as: Who has access to your most critical data? How is access to that data controlled, monitored and logged? How long is that data stored and maintained? How is that data securely destroyed? Ensure that you receive satisfactory answers to these questions.

- Fifth, you should determine whether any Sony-type cyber-incident would be covered by your corporate insurance policies.

- Finally, you should understand your legal rights and responsibilities should such an attack occur. Who in law enforcement or the intelligence community would you contact? What contractual business partners would you be required to notify? What regulatory reporting obligations does your company have? Experience demonstrates that it is much easier to come up with a correct list *before* an incident occurs.

Sony Pictures is only the most recent company to fall victim to sophisticated hackers, as high-profile data breaches at retailers such as Target, Home Depot, and Kmart demonstrate. While no computer system is impenetrable and no internal document or data is ever completely secure from external disclosure, information privacy and security best practices can help mitigate the risks of future cyber incidents. Understanding the principles outlined above – and acting upon them – can significantly enhance your organization's cyber-resilience and, in doing so, fulfill your obligations to shareholders, employees and business partners.

For more information on information privacy and cybersecurity best practices, please contact DeVore & DeMarco at 212-922-9499. We wish you a cyber-safe and happy holiday season!