EMERGING IT RISK (Part of Operational Risk)

In the past several years, ERM and operational risk professionals have been challenged with a new and complex set of IT-related risk. we will review three of these emerging risks: cyber security, cloud computing and social media.

Cyber Security

In March of 2013, James Clapper, Director of National Intelligence, announced that the greatest threat to national security today is no longer extremist terrorism, but cyber crime. This indicates a powerful shift in national paradigm, as the United States moves from the arena of physical threats to cyber attacks. Within the energy industry alone, cyber crime has cost the U.S. economy between $119 billion and $188 billion a year, with the numbers increasing steadily as the attacks intensify.

The U.S. government has categorized cyber criminals into the following tiers, ordered by increasing threat:

Tiers 1 and 2: at these lowest-level tiers, attackers target "known vulnerabilities"

Tiers 3 and 4: with higher levels of funding, these attackers can pinpoint "new vulnerabilities" to exploit

Tiers 5 and 6: funding for these attackers can reach as high as the billions, allowing for the actual "[creation of] vulnerabilities

For the private-sector institution, this rising wave of cyber criminals and the increasing sophistication of their assaults signify the appearance of a new battleground in the form of cyber space, making the issue of cyber security an increasingly integral part of the ERM framework. Former National Security Advisor Tom Donilon voiced his serious concerns about the "targeted theft of confidential business information and proprietary technologies" that has occurred in the private sector, which serves as a Compelling indication of how consequential the concept of corporate data security should be for firms, regardless of their corporate focus.

There are other types of cyber attacks that do not aim to steal information—but this does not mean that they are any less dangerous. For example, a denial-of-services (DOS) attempts to overwhelm a network by flooding its web sites. This paralyzes it, denying users access to the internet and other services, which can seriously cripple a firm's ability to perform essential day-to-day activities. In April of 2013, Charles Schwab was hit by a DoS, and as a result, the company's web site and mobile app were down, then Malfunctioning for two days straight. Schwab spokesman Greg Gabi said that "the denial-of-service had no impact on client data or accounts," but other firms who suffer DoS attacks may not be so lucky.

Just as with other types of risk management, the aim of cyber Security is not to eliminate the threat of a cyber attack, since these are external strikes that are beyond the firm's control. Instead, firms should concentrate on mitigating the damage done by minimizing the amount of data lost. A white paper recently published by Sidley Austin, LLP outlines some key measures that business leaders can take to protect themselves against the theft of intellectual property and other cyber resources. Interestingly, the best method of combating cyber threats is not to completely close oneself off—cyber security becomes more efficient if firms cooperate with each other.

Of course, anti-trust and competition issues make cross-firm collaboration in this manner difficult, with the result that firms have isolated themselves. Understandably, it is hard for private-sector firms to willingly reveal breaches in the hulls of their cyber security frameworks, but note that deliberate concealment of these weaknesses can ultimately backfire. Recognizing the need for a cohesive, guided effort to fight cyber crime, the government has been spearheading efforts to dam up the flood of lost data. However, without the cooperation of private-sector firms through transparent communication, these efforts have been largely frustrated. Tom Ridge, the first U.S. Homeland Security secretary, believes that the biggest barrier to stronger cyber security across the nation is the tense relationship between the public and private sectors, because "the infrastructure that the government relies upon is generally owned by the private sector.''

The government now requires firms involved in "critical infrastructure industries" (namely, finance, transportation, utilities, etc.) to accept the integration of government committees called "information sharing and analysis centers" (ISACs) into their corporate structures. This will increase the availability of cyber-security knowledge, which offers benefits to both the government and private-sector firms. Through the ISACs, the government can support and steer a nationwide defense against cyber crime, while private-sector firms can take advantage of the cyber-security resources of the government.

Adapted from the recommendations given by the Department of Defense (DoD) regard to tightening its own cyber-security measures, here is a list that private firms can use to begin fortifying their cyber shields :

- **Protect Nuclear Strike, Ensure Availability of Conventional Capabilities** : For the private firm, this translates into a need to continuously. test and monitor existing IT systems against cyber attacks. The DoD recommends that nuclear systems should be isolated during testing, and re-designed if necessary: private firms can follow this method of quarantine to improve their ability to contain cyber attacks. It would also be prudent for the firm to review its corporate and legal environments in order to determine the areas most likely to be subject to cyber attacks.
- **Refocus Intelligence**: Here, the DoD recommends a paradigm shift within the department to shift its focus to cyber security as of paramount importance. This applies for private firms as well; cyber security should become a top priority risk with respect to risk policy and risk appetite statements, early warning indicators, and risk monitoring and reporting processes.
- **Enhance Cyber Defenses**: The DoD urges the development of automated cyber defense, which would eliminate the cost of and time needed to manually pinpoint sites of cyber attack—this is also crucial for private firms. Since the government is offering its support, private firms should capitalize on the government's sophisticated cyber-security resources.
- **Change DoD Cyber Culture**: For private firms, this means implementing training programs that ratify the firm's cyber security strategy and teach employees not only how to recognize a cyber attack, but also how to react to one. These training programs may also help to protect the firm from internal cyber attacks in the form of insider leaks.
- **Incorporation of Cyber Requirements into System Lifecycle**: Private firms should consider tailoring their existing cyber security frameworks so that they can be applied to all aspects of the firm, thus ensuring that the company is

protected at all times. These frameworks should also be adaptable, to adjust to different forms of cyber attack.

Above all, it is important to realize that the constantly occurring advances in technology make cyber crime a dynamic and fluid challenge that is Perpetually evolving. For example, computer networks are no longer the only sites of vulnerability—cyber criminals are now switching their targets to software and hardware that have yet to be integrated into the technological framework of private-sector firms, which expands the threat to the manufacturing process as well. Hence, it is essential for a firm's risk management framework to be flexible and to be constantly adapted to meet the cyber crime threat.

Cloud Computing

Cloud Computing, which derives its name from the popular use of a cloud to symbolize the complexity and comprehensiveness of a cloud system allow firms to use external cyber resources (such as hardware, software, and data). Not only does cloud computing allow firms. to significantly reduce overhead costs by reducing the capital needed to invest in physical and electronic storage, cloud computing can also help firms to update their own IT environment, and so improve the firm's overall flexibility and efficiency. A recent Rackspace study shows that cloud computing increased profits by an average of 22 percent and saved companies an average of $478,300 on IT expenditures.

Firms can choose to implement cloud-computing services internally, access a cloud system through external service providers, or pursue any combination of the two:

- **Vendor clouds** are sold by external cloud service providers (CSPs) and allow the firm to access resources, shared with other customers, through the internet (or other form of network).
- **Private clouds**, which are modeled after vendor clouds, are managed exclusively by and can only be accessed from within, the firm itself.
- **Hybrid clouds** combine vendor clouds and private clouds to provide a cloud structure that can be tailored to fit the firm's needs.
- **Community clouds** are used by firms - normally within the same industry—that share goals and interests and can be internally or externally managed.

Despite the many cost advantages of cloud computing, it does not eliminate the risks associated with these resources pre-cloud implementation, nor does it contribute significantly to a firm's efforts to tighten cyber security, as we previously discussed. In fact, cloud computing brings with it a new set of risks, stemming mainly from a dilution of management's control over the firm's data.

The use of vendor clouds makes firms particularly susceptible to increased risk, because they are now also exposed to the risks experienced by the CSP's other customers, as well as the CSP itself. Neither the CSP nor the other customers are likely to make efforts to align their own risk management frameworks with that of the firm or engage in transparent communication about internal processes. This causes complications in risk management because we must now consider potential divergences in interest. Ultimately, the firm virtually ties itself to these third parties, which can threaten the stability of the firm's IT environment.

Cloud computing can also make the firm a more attractive target for cyber criminals, because they only need to infiltrate one network in order to gain access to the cyber resources available on that particular cloud. As such, the risk of data leakage—whether externally through cyber criminals or internally insider leak—increases significantly when a firm shifts considerable amounts of private data onto a cloud system.

However, applying risk management strategies to cloud computing can allow a firm to harness its true potential without sacrificing data control. These strategies are concepts that we have seen before: the definition of appetite statement, a robust model for governance, strong, defined pathways of communication, and a thorough grasp of the firm's current IT environment. Most importantly, the firm's risk management framework should be adjusted to also encompass the risk universes of the CSP and the CSP's other consumers in order to give the firm a more complete vision of its own new risk universe.

Social Media

The rise of social media has changed the business world in profound ways by ushering in an unprecedented improvement in the ease of community building, communication, and knowledge transfer. However, social media can be a double-edged sword for firms that do not fully comprehend its far-reaching potential in influencing key stakeholders' perceptions of the firm, especially in crisis situations.

Within the institution, social media can significantly impact the relationship between employees and the corporate environment because it obscures the line between personal and corporate boundaries. Firms that allow the uncontrolled use of social media during the workday risk experiencing a decrease in employee productivity as employees become distracted and lose focus. A recent Mashable study reveals that some form of social media interrupts employees every 10.5 minutes—this translates into a loss from the entire U.S. economy of close to $650 billion.

Social media can also compound employee loyalty problems and increase the chance of an insider leak, particularly as more employees become disenchanted with management. Even in cases where employee loyalty is unshakeable, the lack of restriction in social media channels can encourage unintentional information breaches. On that note, the introduction of social media into the workplace has also amplified the risk of cyber attacks, since social media platforms are thriving hotbeds of active viruses and malware, which can very easily be downloaded onto the internal network by an un-suspecting employee.

Social media also plays a key role in shaping the relationship between the firm and the public, and can make or break the firm's brand image. Platforms like Facebook allow firms to directly interact with their customers-for better or for worse. for example, in March of 2010, Facebook users attacked Nestle's Facebook page after Greenpeace harshly condemned the Company for its use of palm oil in its candy products. Nestle's attempts to contain the negative feedback by closing the page to comments only fanned the flames by drawing attention to the incident.

The Nestle case demonstrates the importance of social media in not just selling products, but also in building relationships with consumers. Nestle could have taken advantage of its Facebook page by using it to provide an explanation or the rationale behind its use of palm oil to the public, which may have lightened the impact of

Greenpeace's campaign against Nestle. Utilized properly, social media platforms can actually be risk management tools because they provide early warning indicators of emerging stories and issues and the ability to communicate with stakeholders. As it was, Nestle's misuse of Facebook only deepened the public's perception of the firm's culpability.

The first step to managing the risk associated with social media is to realize that social media affects the entire corporation, and is not simply limited to the IT department. As such, all efforts to broaden the existing risk management framework to include social media should be led by a team comprised of individuals from all sections of the firm and all levels of management. From this point on, we can then, for example, develop a social media policy that specifies the permitted and banned activities with respect to work time and company IT equipment. It would also be prudent to constantly monitor social media channels to identify emerging narratives and themes, as well as to intervene in any backsliding of the firm's public image.