INAUGURAL GC TALK SERIES

BLURRING THE LINES

The legal function of a company has a critical role to play along with the IT department in safeguarding an organisation from cyber threats and attacks.

It is evident from recent high profile attacks on large and small corporations that cybercrimes and breaches have a serious impact on the reputation and financial standing of organisations. Often, the general counsel is the last to arrive at the crime scene. What can in-house counsel do to counter internal and external cyber threats? ***the Oath*** in association with ***Akin Gump*** organised the first breakfast seminar in the GC Talk Series and focused on 'Cyber Security & the GC' – how general counsels and their teams can implement practical measures to enhance the cyber security of the organisation. Natasha Kohne, co-managing partner of Akin Gump Abu Dhabi, led the interactive discussion.

Kohne began the discussion sharing her observations based on current developments in the cyber security and data protection space that include unprecedented changes globally especially in the US and Europe, increased regulatory scrutiny, the issue of privacy versus security, old laws lacking applicability to new technology among others. "Even though we have seen more awareness of security among organisations, attackers have become more sophisticated and some company practices are not effective enough to withstand such breaches," noted Kohne.

EXAMPLES OF HIGH PROFILE SECURITY BREACHES

She went on to discuss a few examples of how recent cyber security events within the last six months demonstrate the speed at which the industry is moving.

- Apple vs. US Department of Justice – This is an example of the tension between security versus privacy and civil liberties. The U.S. Department of Justice asked Apple to develop a software that would unlock the iphone of the San Bernardino, California mass shooter without deleting the iphone's contents. Apple fought back, arguing that the development of a software to circumvent the iphone's security feature would permit further exploitation. The court did not have to resolve the case as the US Department of Justice paid an unknown source to unlock the iphone. Panama Papers – Arguably the world's largest data breach to date that may have serious implications involving tax disclosure, anti-money laundering, bribery sanctions, reputation and civil liability concerns. The incident also demonstrates increased vigilance toward careful entity structuring and third party vendor relationships.

- EU General Protection Regulation (GDPR) – This is considered to be one of the most significant updates to the EU privacy law in two decades. It was signed by the EU Parliament in April 14, 2016 and will come into enforcement in July 2018. It will have a major impact on how businesses collect, store and use data binding all 26 EU states and harmonises data protection rules. Kohne added, "Penalties are harsh as it could be up to four percent of a company's global revenue. UAE companies need to take note of this extra territorial law as it may apply to EU citizens in your organisation."

- Safe Harbor – As per the EU's Data Protection Directive 95/46/EC prohibits the transfer of personal data from Europe to a third country, unless that country "ensures an adequate level of protection." In 2000, the US negotiated the Safe Harbor framework, which the European Commission found "adequate." The Safe Harbor was a self-regulatory framework where companies could register with the US Commerce Department and self-certify that their data protection practices were adequate. About 4,400 companies were using the Safe Harbor. However, in October 2015, the European Court of Justice found that the Safe Harbor was inadequate to protect the privacy right of EU citizens. In Feb 2016, EU Commission and US announced that there was a new framework agreement for transatlantic data flows, but the new framework still in approval process

- Bangladesh Central Bank Cyber Attack – According to reports, attackers used malware to get into the system and watch how the central bank withdrew money from its US account. Using the Bangladesh Bank's SWIFT code, hackers were able to successfully request the Federal Reserve Bank of New York to transfer millions of dollars. Kohne highlighted, "This is one of the many examples of banks around the world being attacked. In the US especially, banks are responding. After suffering a critical breach, for example, one large US bank announced that it would spend USD500 million in 2015 and would continue to double spend over the next five years. We are seeing banks hiring former FBI agents, military advisors and so on to advise on these issues. Banks are more actively suing players in the retail and hospitality sector for data breaches that may have happened due to negligent data security practices of such companies."

WHAT DO THE STATISTICS SAY?

Based on a first of its kind report, the Association of Corporate Counsel (ACC) issued, 'The State of Cyber Security Report: An In-house Perspective', Kohne reflected on some key findings in the report, including that reputation is the top concern worldwide when it comes to cyber security and employee error is cited as the top cause of breaches.

WHAT IS REASONABLE SECURITY?

The definition of reasonable security and how companies can decide the adequate level of security is often a key issue. Kohne discussed the internationally accepted National Institute of Standards and Technology (NIST) framework, "The Core is not a checklist of actions to perform. It presents key cyber security outcomes identified by industry as helpful in managing cyber security risk." There are five primary functions – Identify, Protect, Detect, Respond and Recover. Kohne gave other examples of jurisdiction attempting to identify what "reasonable security" is, "The State of California has one of the most cutting edge privacy and security regimes. Recently, California identified the Center for Internet Security (CIS) Critical Security Controls as a baseline standard for the 'minimum level' of security companies must maintain," said Kohne.

WHAT IS THE ROLE OF THE GENERAL COUNSEL?

Cybercrime is a force to be reckoned with and one that transcends the IT department of companies. It

has become critical for the in-house legal function of an organisation to play a vital role to mitigate cyber risks. "Lawyers play an important role not just in mitigating a cyber-breach but also once a breach occurs. Once a breach has happened, you should focus on containing, mitigating and remediating the attack as much as possible." Kohne identified communication as one of the top challenges of cyber security. "For those who are not familiar with building IT infrastructure, it helps to sit down with the IT head of your company and understand how he or she approaches building a multi-layered defense…" Kohne said that the most important tool to prepare for a cyber-breach is an Incident Response Plan – develop the plan, evaluate with the board and test regularly through mock-breaches.

Build a cyber security compliance framework

Kohne mentioned that the approach to cyber compliance can be similar to building other compliance programs. Akin Gump undertakes a five step compliance process that includes conducting a gap analysis, a corrective action plan and proper implementation and monitoring. Kohne recommended that the compliance framework should also include dealing with employee-related breaches. She shared some of the cutting edge tactics that companies are using to engage employees and develop a culture of security. An approach to vendor management must also be a focus considering that third-party breaches were a main concern in the Middle East.

Third-Party Vendor Management

Going around the room, the in-house counsel raised the concerns of dealing with third-party vendors as they can be responsible for a large number of breaches. Kohne stressed the importance of careful due diligence at the pre-contractual stage and ensuring effective monitoring and auditing processes throughout the relationship.

BLURRING THE LINES BETWEEN IT AND LEGAL

The common challenge between IT and Legal is the lack of understanding on either side of the technical and legal obligations involved in a data breach. Kohne explained the importance of both sides meeting at a middle ground to mitigate this risk and bridge the gap. "Being trained on IT terms can help a lawyer to come up to speed on the IT framework of the company. Lawyers are trained specifically to analyse and distill complicated information – use this skill and legal knowledge to create a comprehensive cyber security program for your organisation along with the IT department. It is important to have this two-way conversation," recommended Kohne. "You cannot prevent a breach. The key lies in how a general counsel mitigates, responds and remediates. How quickly you respond and remediate can be the difference between a minor breach and a major disaster."

KEY TAKEAWAYS

Kohne identified multiple takeaways to being compromise ready, including:

- Implement a comprehensive cyber security compliance program;
- Develop and annually test your Incident Response Plan;
- Undertake a data mapping analysis and protect your organisation's most sensitive data;
- Address key concerns arising out of annual risk assessments;
- Analyse third-party access to data and your legal relationship and obligations; and
- Assess cyber insurance coverage.

General counsel are and will increasingly continue to play a key role in protecting an organisation.

Event Series

the Oath GC TALK SERIES

In Association with

Akin Gump
STRAUSS HAUER & FELD LLP