TX Office: (817) 416-6842
NV Office: (702) 565-2727

Kral Ussery LLC
Certified Public Accountants
Advisors - Litigation Support - Internal Audit

June 23, 2021

Ransomware Themes Keeping Directors Up at Night

Board Education & Oversight Involvement is a Must

By Ron Kral, CPA, CMA, CGMA
Partner of Kral Ussery LLC

If it isn't already, cybersecurity should likely be on your board agenda at every meeting. Board involvement is critical as outlined in one of my previous articles - *The Importance of a Cybersecurity Strategy*. Read further for additional themes directors should be thinking about.

Increased Risk

The global COVID pandemic has created an environment where companies have moved toward rapid network expansion and deployment of remote devices to support telework, which has provided more opportunities for cyber-attacks specifically associated with ransomware. Attackers identified the expanded attack surface, which includes lack of VPN implementation, increased third-party and vendor access, and use of cloud services, as examples of areas where security was not as robust as needed. Attackers have taken these opportunities and leveraged a "ransomware as a service model" because it results in payments from victims faster than stealing and selling data to other market participants.

There is even collaboration between hackers in that they may purchase or exchange access to information and subsequently hold data ransom or extort companies with threats to sell or publish the stolen data. Data exfiltration is increasingly part of ransomware attacks, which is more sophisticated and detrimental to companies as it allows for further exploitation opportunities, even if a ransom is paid. Systems are compromised through phishing schemes targeting employees who unknowingly download malware. Email schemes like these along with phone calls or text messaging to executives ("smishing" schemes) have drastically increased over the past year. All of this at a time when not only are companies trying to keep up with network vulnerabilities resulting from technology expansion, but are also dealing with resource constraints throughout all levels and departments.

Continuous Preparation Is a Board's Best Defense

Current boardroom "wargames" (cyber threat scenario planning) may be falling short in protecting companies from hackers. The "destroy your business" exercises now need to expand from a competitor focus to include critical infrastructure and data protection risk, and these need to be continual exercises as the bad actors become increasingly more sophisticated. Some specific organizational considerations include:

- **Drafting and practicing an incident response plan** – It is not enough to have a plan developed, it needs to be practiced, questioned and revised as part of the "lessons learned" that is an outcome from testing and practicing the plan.

- **Business disaster recovery communication process** – Develop it, implement it and practice it. This process should include how and who to communicate with at varying phases of the process. Educating those involved as to why these boundaries exist will assist in proper execution (e.g., mitigate reputational damage, comply with contractual requirements and legal statutes, etc.).

- **Continuing education for all professionals** – It only takes one human error to give a hacker access to a company's data. All employees must be continually educated and tested through regular phishing exercises, awareness campaigns, mandated training or even security focused trivia/contests. Involving experts in this process may be time and money well spent.

- **Cyber incident exercises** – Again, practice makes perfect, and while no company will ever achieve perfection, active preparation including varying real-world scenarios throughout the company and inclusion of various stakeholders, may significantly aid a company in preventative and detective measures.

- **Create a culture of awareness and reporting** – Culture shapes the desirable attitudes and behaviors of an organization's personnel. Incorporating core values that promote awareness and reporting of wrong doings or threats will go a long way in safeguarding the organization and its stakeholders.

- **Robust and timely threat data** – Boards and management need to have timely and appropriately robust information about significant risks impacting the business. Providing the Chief Information Security Officer (CISO) or similar role within the organization with appropriate resources, funding, and support should enhance the security makeup of the company. Another common practice is for the CISO role to report directly (and regularly) to the board to enable proper management and prioritization of risk.

- **Adequate insurance coverage** – Another common theme is: It isn't a question of *if*, but rather *when* a cyber incident will occur. The purpose of insurance is to help offset financial losses when a cyber-attack happens. It is critical to regularly (at a minimum of annually) review policy coverage, as not all policies are created equal and risks continue to rise and may be scaled based upon the nature of the target. The ransom payments can vary depending on the type of attack. Multi-million-dollar ransom payments are not uncommon for resolving ransomware matters, and have been as high as $4.4 million for the ransom paid by Colonial Pipeline. Through the final quarter of 2020, ransom payments, on average, were approximately $154,000 (Coverware, February 2021). This average is expected to increase for 2021 in light of some of the high-profile ransoms recently paid.

Included below is a short list of considerations as a starting point to assist in company planning. While each company will have its own risks, risk appetite, and mitigation techniques that are taken into consideration, the list below should aid in the thought process. The process of identifying, planning, rehearsing and adjusting is never finished and is an iterative cycle. Cybersecurity is an ever-changing landscape that requires continued oversight, updates, education and guidance.

Managing Cybersecurity Requires a Layered, Risk-Based Approach

Board oversight is critical in the management of cybersecurity as a whole, but especially for ransomware, since the increase in attacks year-over-year is up as much as 715% according to a study by Cyber Florida at the University of South Florida. The board should question and challenge management, identify where additional expertise and experience may be needed, and help determine the adequacy of resource allocation and processes – both financial and human. In performing these

duties, the board needs to understand the layers of defense available to mitigate ransomware risk and design their responses to the threats accordingly.

- **Inventory and Evaluation** – This layer includes understanding data, devices and third-party vendors that are part of the company's daily processes. Action items include data mapping, data classification, user access, application inventory, device and IoT inventory, and vendor risk management programs. Creating this mapping and inventory is used to gain an understanding of the company's potential gaps, where the risks may exist, and what mitigating factors are in place or need to be added to reduce the risk of a breach or other security issue.

- **Prevention** - There are *multiple* layers of prevention against an imminent breach:
    - **People** - The training and assessing of those with access to company assets and data is critical. Similar to the board exercises mentioned above, employees, contractors and in-scope vendors who connect to company systems should be trained on the company policies and standards to reduce risks and enhance response times. Of course, this implies that organizations have current policies and standards to address cybersecurity risks. If not, this needs to be a priority. Testing scenarios should also be scheduled and conducted, such as mock phishing emails to a sample of all in-scope personnel and/or third-party vendors.
    - **Email Security** – Using technology can assist employees with their diligence and commitment to helping prevent an adverse activity, such as phishing. Solutions may include spam filters, central tools scanning emails and attachments, strong password requirements, required connectivity approvals for company devices, or mandatory security solutions installed on non-company devices.
    - **Remote Connectivity** – Companies need to remain diligent regarding network and remote connections and have solutions in place to search for the weakest link in their structure, which may include remote connections and third-party access – e.g., supply chain. Remote connectivity should require two factor or some form of MFA (multi-factor) technology for all connections to company systems or to third-party hosted solutions that contain company applications and/or data.
    - **Perimeter** – Preventative measures that are necessary to reduce the risk of a compromise to the systems include firewalls, endpoint security, cloud security and patching. Additional items to consider that can help address security needs include documenting policies and operational procedures, implementing data encryption, performing data destruction, monitoring network activity, and implementing network segmentation.

- **Detection** - How and who will identify a breach in security? The longer a compromise goes undetected, the more likely the attacker can establish a foothold, escalate privileges and expand their presence within an organization to ultimately exfiltrate data and potentially maintain a longer-term presence. Automated security, monitoring and detection solutions, robust access controls, and human oversight all need to be part of the process to create a layered approach that enhances the ability to block, detect and isolate issues.

- **Recovery** – This layer includes the detailed response and communication plan. The plan should be tested and rehearsed at least annually. Another important aspect of recovery includes evaluation of the company's data backup plan. Hackers have begun to start locating the backup solutions on the network and compromising the process intended to help with the potential recovery and mitigation process.

Timing Is Everything - Immediate Action Is Critical in Responding to Ransomware Attacks

Ransomware may have significant impacts within hours or even minutes upon the initial compromise leaving very little reaction time. Couple that with hackers timing their action during off-hours, weekends or holidays in the hopes of dodging detection, which can result in a longer period of time to cause more significant issues. Identifying the signs and signals of an attack requires the company to stay a step ahead of hackers, be vigilant and continually revisit and revamp strategies to secure the company's assets.

Companies must be prepared and confident in reacting to an attack upon being identified in a timely manner. Scenario based rehearsal on a regular basis helps with this preparedness. Additionally, many companies have limited experience with cyber-breaches, which may require the board to assist in identifying and providing external expertise to fill this gap. Regardless of where the experience and expertise resides, a leader should be designated for the recovery process, and a response plan that include specific roles, responsibilities, policies and communication plans needs to be in place.

Fighting Cyber-Crime Takes a Village

To help improve the security posture, companies need a multi-pronged approach to combat cyber issues. Gaining ground against attackers may require government involvement and industry unity, in addition to the individual company's efforts.

- **Internal** - A company needs all employees to be dedicated and diligent in the protection of company systems and data. Starting with the tone at the top, the culture must promote and provide for awareness of the diligence and urgency required when it comes to cybersecurity. A few items to include as part of the company awareness process are:
    - Identifying and ranking the top enterprise risks for the organization
    - Allocating funds or creating a budget for on-going security needs
    - Monitoring industry trends or preventative activities that can help reduce the risk of a breach or attack

- **Board** - The board needs to make cybersecurity a priority by requesting frequent briefings (at least quarterly and as needed on a real-time basis) and assigning responsibility to either the full board or to an engaged committee within the board that reports regularly to the full board. When expertise is not available within the board, it is important to acknowledge that outside advisors may be needed.

- **Governmental Authority** - Similar to society's reliance on government protection from a variety of unlawful activities, support should be requested in the cyber realm. Government coordination, including the Federal Bureau of Investigations (FBI) and Department of Homeland Security (DHS), is often critical in ransomware breaches. The U.S. Department of Justice (DOJ) and the Cybersecurity and Infrastructure Security Agency (CISA) are additional federal authorities teaming with allies in this area. In January 2021, international collaborative teams seized control of the computing infrastructure used by Emote, a botnet of infected machines that has been one of the most pervasive cybercrime threats over the last several years. But, as with internal cybersecurity, these efforts must continue and increase to counter rising cyber-crime activity.

- **Industry** - Industry leaders may gain efficiencies by having a united front against cyber-crime, especially given the industry specific circumstances associated with ransomware attacks. Industry leaders may share experiences and information with peers and governmental agencies to help inform and provide protection based on known issues. Industry groups may

further unite in lobbying for support from cryptocurrency managers and exchanges, which is a favored method of payment in ransomware attacks, to join the fight.

Conclusions

Understanding the risks and solutions of cybersecurity is critical for directors in meeting their fiduciary duties of care and loyalty, which includes the subsidiary duties of good faith, oversight and disclosure. This doesn't mean that all directors need to become cyber-experts, but ideally at least one independent director should have significant knowledge in this area. Collectively, the board and their committees should possess enough knowledge to help guide management and provide adequate oversight to help ensure that cyber-risks are being addressed. Having a strong internal audit function and tapping into third-party advisors can go a long way to help directors meet their fiduciary duties pertaining to cybersecurity.

*****

Ron Kral is a partner of Kral Ussery LLC, a public accounting firm delivering advisory services, litigation support and internal audits. Ron is a highly rated speaker, trainer and advisor. He is a co-author of *The Board of Directors and Audit Committee Guide to Fiduciary Responsibilities: Ten Critical Steps to Protecting Yourself and Your Organization*. Ron is a member of 4 of the 5 COSO sponsoring organizations; the AICPA, FEI, IIA and IMA. He can be contacted at rkral@KralUssery.com or www.linkedin.com/in/ronkral.

Kral Ussery LLC serves US public and private companies to protect and grow shareholder value, as well as non-profits and governments with internal controls and in combating fraud. We assist entities with governance and in all matters relating to financial reporting, including SEC compliance, internal controls testing and remediation, IT general controls, IPO/SPAC readiness, M&A transactions and US GAAP. Visit us at www.KralUssery.com.

This is an article from the Governance Issues™ Newsletter, Volume 2021, Number 3, published on June 23, 2021 by Kral Ussery LLC.