



**FIVE RANSOMWARE
THEMES KEEPING
DIRECTORS UP AT NIGHT**

Spoiler alert: If it isn't already, cybersecurity should likely be on your board agenda at every meeting. BDO recently hosted directors and subject matter experts at regional board roundtables to learn, mentor and network among peers on the topic of ransomware. Here are the top five takeaways from our recent discussions.

Contents

INCREASED RISK	1	TIMING IS EVERYTHING- IMMEDIATE ACTION IS CRITICAL IN RESPONDING TO RANSOMWARE ATTACKS	4
CONTINUOUS PREPARATION IS A BOARD'S BEST DEFENSE	2	FIGHTING CYBER-CRIME TAKES A VILLAGE	5
MANAGING CYBERSECURITY REQUIRES A LAYERED, RISK-BASED APPROACH	3		

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 cyberattacks 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, and it doesn't stop there. 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. 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 never 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/support to perform assigned duties 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 Ryuk associated issues, and have been as high as \$1.4 million ([MSSP Alert, April 30, 2020](#)). Through the final quarter of 2020, ransom payments, on average, were approximately \$154,000 ([Coverware, February 2021](#)).

Within this document is a short list that has been put together as a starting point to assist a company in planning. While each company will have its own risks, risk appetite, and mitigation techniques that are taken into consideration, the list is simply intended to aid in the thought process. The process of identifying, planning, rehearsing, and adjusting is never finished and is an iterative cycle. Technology and the corresponding security 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. 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 processes. Testing scenarios should 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 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 once it has been identified. 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 includes 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

The board also needs to make cybersecurity a priority by requesting frequent briefings (at least quarterly, or even monthly) 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 six 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.





To learn more about BDO's resources in the cybersecurity, data privacy and digital transformation space, visit [BDO Digital](#). For additional thought leadership and educational opportunities on dynamic issues facing corporate directors, we invite you to subscribe to [BDO's Center for Corporate Governance and Financial Reporting](#).

CONTACT US

GREG SCHU


Partner, Government, Risk and Compliance
612-367-3045 / gschu@bdo.com

KAREN SCHULER

Principal, Government, Risk and Compliance
301-354-2581 / kschuler@bdo.com

AMY ROJIK

National Assurance Partner
617-239-7005 / arojik@bdo.com



BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 65 offices and over 700 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 88,000 people working out of more than 1,800 offices across 167 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2021 BDO USA, LLP. All rights reserved.