Spotlight on Cybersecurity and Ransomware Attacks

This presentation is being made based on the understanding that an attorney-client relationship does not exist between you and Kirkland & Ellis and will not exist unless and until we execute an engagement letter. Additionally, nothing that occurs (including if you provide us with information) before the execution of an engagement letter will preclude Kirkland & Ellis from representing others with interests adverse to you in this or any other matter. Any representative matters and other experience included herein may date from periods before an individual lawyer joined Kirkland & Ellis, may contain incomplete or colloquial client or entity name references, and should not imply current or former client status. None of these materials is offered, nor should be construed, as legal advice. Prior results do not guarantee a similar outcome. © 2021 Kirkland & Ellis LLP. All rights reserved.

Cybersecurity and Ransomware – Overview

As reflected in recent headlines, public and private sector entities face malicious cyber activity from both nation-state actors and cyber criminals, increasingly resulting in high-profile ransomware attacks

- For example, JBS, the world's largest meatpacker, was subject to a ransomware attack that on June 1 forced the shutdown of all its U.S. beef plants, leading to an $11M ransomware payment

In recent years ransomware attacks have become increasingly sophisticated and crippling to businesses

- In the past, many hackers would employ a strategy to install malware that would then encrypt company servers, and offer decryption keys in exchange for a ransom with the hacker never gaining access to company information
- More recently, attacks are also focused on exfiltrating sensitive company information. In addition to deploying malware to encrypt company systems, attackers threaten to publicly expose valuable intellectual property or other confidential information

Cyber risk and deficiencies are an increasing focus of regulators

- On June 15, 2021, the SEC announced settled charges against an issuer for disclosure controls and procedures violations related to a cybersecurity vulnerability that exposed sensitive customer information
- Issuer filed an 8-K detailing a cyber incident, but the responsible executives were not informed that IT had identified the vulnerability several months earlier and failed to remediate it per company policy

The White House is taking an active role in improving cybersecurity

- On May 12, 2021, President Biden issued an Executive Order focused on improving the nation's cybersecurity and federal government networks
- On June 2, the White House issued a memo to business leaders titled "What We Urge You To Do To Protect Against The Threat of Ransomware", urging immediate steps to protect against the threat of ransomware

Recent developments reinforce that boards and company management should focus on key issues to consider before, during and after a ransomware attack

~2,400

Victims of ransomware in 2020; U.S.-based governments, schools and healthcare

77%

Ransomware attacks in Q1 2021 involved the threat to leak exfiltrated data

$40M

CNA Financial ransomware paid to regain control of its network after a cyber attack

$350M

Victims paid in ransom in 2020 – a 311% increase over the prior year

21 Days

Average downtime due to ransomware attacks

287 Days

Average days it takes a business to fully recover from an attack

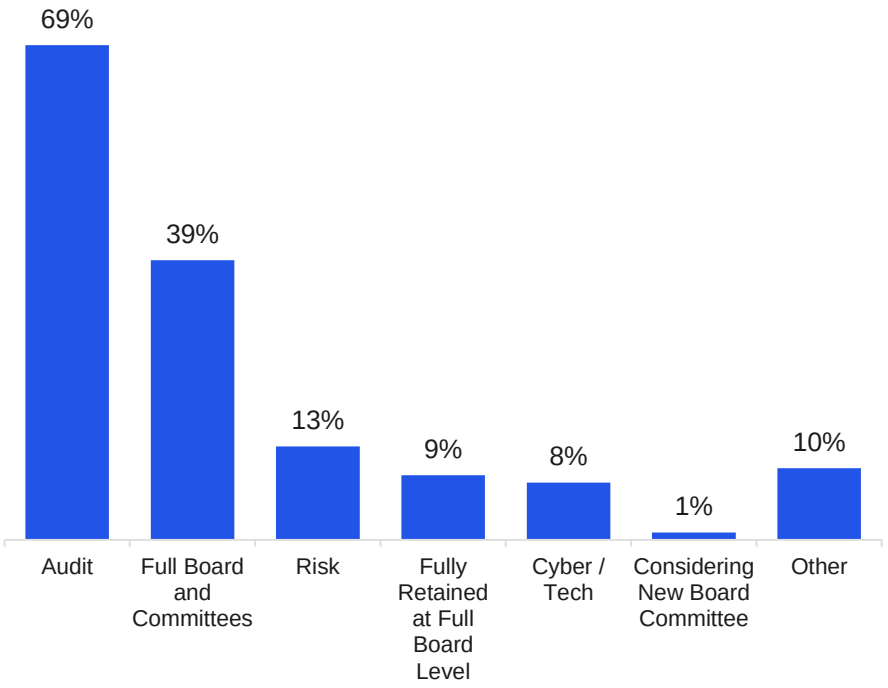
Sources: Wall Street Journal, Coveware, Emsisoft and Chainalysis

Cybersecurity Board Oversight

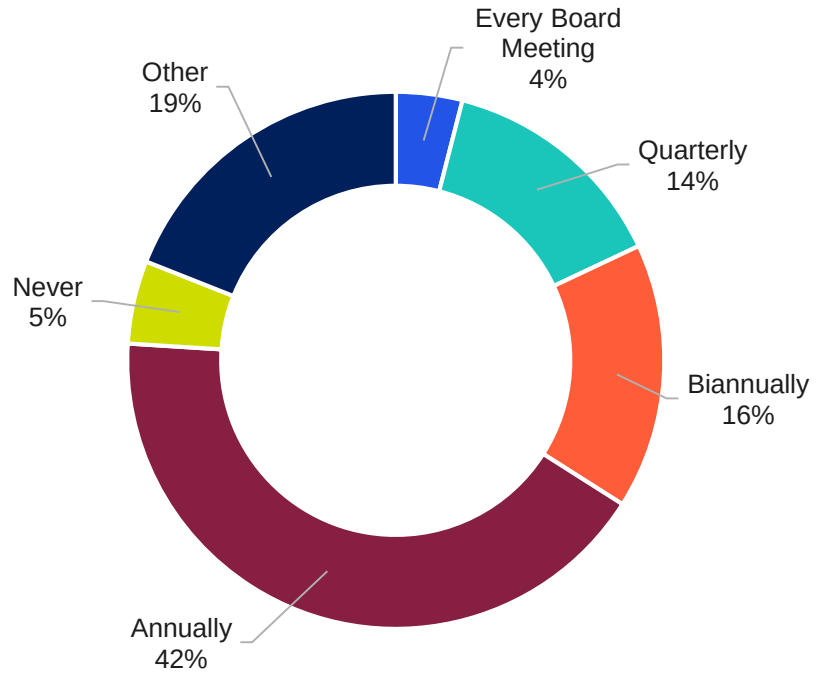
Boards should consider with management the appropriate oversight for cybersecurity risk

- While oversight may be provided by the full board, it is common to delegate cyber risk oversight to the audit committee
  - In some cases boards are electing to form a dedicated, cyber-specific board-level committee or sub-committee
- Regardless of the approach, boards should consider including cyber risk as a recurring agenda item for full board meetings, including regular director education on cyber risk developments
- Board should also consider experience in technology / cyber risk as part of refreshment assessments with a focus on experience to oversee a comprehensive cybersecurity readiness plan

BOARD COMMITTEE RESPONSIBLE FOR CYBER RISK OVERSIGHT*
(select all that apply)



FREQUENCY OF CYBER RISK ON BOARD MEETING AGENDAS*
(vs. committee level)



* Source: Society of Corporate Governance – based on responses from a March 2021 survey of ~110 public company respondents – report here

Minimizing Your Company's Exposure to a Ransomware Attack (1/3)

In addition to the IT security considerations (including the recommendations by the White House – see following slides), companies should consider the following to protect against the likelihood and severity of cyber attacks

BEFORE A RANSOMWARE ATTACK	
Resources, Policies and Reporting	▸ Companies should consider evaluating cybersecurity and internal audit functions to ensure they are appropriately resourced with personnel with the necessary cyber risk-related technical expertise ▸ Companies should consider written policies and procedures governing the cybersecurity framework and regularly assess their reporting systems and processes to ensure effective oversight
Cyber Insurance	▸ Companies should consider obtaining cyber liability insurance, which can cover the cost of responding to a ransomware attack (e.g., counsel, forensics IT firms) and remediating the IT environment, as well as fees or liability from resulting lawsuits – For companies with a cyber insurance policy, review to confirm scope and level of coverage ▸ Companies should also consider whether existing insurance policies (e.g., property or business interruption policies) cover cybersecurity incidents, particularly as the largest costs of cyber-attacks are often related to business interruption ▸ Be prepared for more expensive cyber insurance (and renewals) given the increasing frequency of ransomware attacks and the increasing cost of the ransoms demanded (premiums were up 22% in the U.S. in 2020, per Fitch Ratings) and potentially more limited coverage in sectors deemed high-risk (e.g., where companies collect highly sensitive data)
Incident Response Plan	▸ Establish an incident response plan ahead of time. Review the CISA library of ransomware prevention best practices and response checklist when developing an incident response plan, which should consider: – The minimal IT infrastructure required to run the business. For example, a company might be able to take orders on paper but might not be able to function without certain systems – How company personnel can communicate if email is unavailable. Consider establishing an emergency phone tree or a secure texting app so that senior management can communicate if company email systems are down – The role and selection of potential external "first responders." In addition to the management team, consider including legal counsel, a forensic IT specialist, a crisis communications firm, a company's insurance carrier, and a consultant that can acquire cryptocurrency and arrange to make a ransom payment if necessary – Delegate person(s) to be single point of contact for communications with the hackers and media inquiries ▸ Consider conducting tabletop tests of the incident response plan

Minimizing Your Company's Exposure to a Ransomware Attack (2/3)

DURING A RANSOMWARE ATTACK	
Notify the Team	▸ In the event of a ransomware or other cyber extortion event, companies should follow their written incident response plan, in particular notifying the core advisor / management team and potentially the board ▸ Consider communicating via secure messaging app If there is a risk that company email is being monitored ▸ Depending on the severity of the incident and other factors, consider notifying the FBI / other law enforcement
Preserve Right to Coverage Under Cyber Insurance	▸ Companies that are victims of a ransomware attack should notify their cyber liability carriers - failure to do so can preclude coverage for certain expenses, such as fees for legal counsel or forensic IT specialists ▸ Some policies also require the policyholder to inform applicable law enforcement agencies prior to providing coverage for any costs incurred and many require prior approval of the ransom payment
Be Mindful of Privilege	▸ Appropriately involving counsel wil reduce the risk of exposure of otherwise privileged materials in any class-action lawsuits or other legal claims that may be brought in the wake of the data breach ▸ In particular, consider having counsel engage the forensic IT specialist and any others conducting an investigation
Whether to Pay the Ransom	▸ Whether to pay a ransom is fact-specific and ultimately sits with senior management and often the board. Factors to be considered include: – To what extent is the company able to operate without paying the ransom? – Does the company have other access to the exfiltrated information (i.e., offline backups) and how sensitive is that information (i.e., what are the risks of its disclosure)? – Do the costs of a business disruption, the impact to systems or customers, negative publicity or reputational harm, exceed the ransom demand? – Do the attackers have a track record of providing a working decryption key and not promulgating follow-on attacks? – What is the size of ransom demanded and is it recoverable from insurance? ▸ Note that the FBI has stated that its policy and guidance is that companies should not pay ransoms and that quickly contacting law enforcement opens up the possibility of creative solutions ▸ Before making a payment, companies need to consider whether doing so would violate U.S. law prohibiting payments to individuals or entities that are subject to U.S. economic sanctions or that are designated as terrorist organizations – While the odds of conclusively determining an attacker's identity may be low, companies and their counsel should nevertheless conduct diligence on the attacker's identity (including based on the attacker's cryptocurrency wallet) to seek to determine whether such a payment would violate U.S. law

Minimizing Your Company's Exposure to a Ransomware Attack (3/3)

AFTER A RANSOMWARE ATTACK	
IT Monitoring	► Many forms of ransomware embed themselves deep in a company's systems in order to launch future attacks ► Even after paying a ransom and applying a decryption key, or after restoring the systems from backups, companies should consider monitoring their systems and network for potential reinfection attempts by the ransomware ► To help prevent future attacks, companies should consider reviewing their IT security environment for other potential active threats, while also reviewing their security controls for potential enhancements
Notifications / Disclosure	► Legal counsel can advise on whether companies are required to notify employees, customers, investors, regulators, or others of the ransomware attack. Even if such notification is not legally required, companies should consider whether notification is nevertheless appropriate as a business matter ► In particular, consider whether the incident requires public disclosure in SEC filings
Record Keeping	► Companies should consider reviewing their documentation of the board and committee oversight activities regarding the incident to ensure they accurately reflect the oversight involved
Litigation and Enforcement	► Companies that are victims of ransomware attacks historically were not the subject of follow-on civil litigation or government enforcement actions. However, the trend has changed in recent years, with an increasing number of lawsuits and government investigations ► Many of these actions are pending, so their success is to be determined. However, we expect that shareholders and other stakeholders will demand greater protection from companies if and when an incident occurs ► As such, we anticipate that litigation, government investigations, and enforcement actions related to ransomware are likely to rise in the coming months and years

White House Memo on Protection Against Ransomware

On June 2, 2021, the White House released a memo issued to corporate executives and business leaders with the specific recommendations below to protect against the threat of ransomware



THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

Backup Data, Test Systems and Keep Backups Offline	▸ Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups ▸ Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems
Update and Patch Promptly	▸ This includes maintaining the security of operating systems, applications, and firmware, in a timely manner ▸ Consider using a centralized patch management system; use a risk-based assessment strategy to drive your patch management program
Test Incident Response Plan	▸ There's nothing that shows the gaps in plans more than testing them: Are you able to sustain business operations without access to certain systems? For how long? Would you turn off your manufacturing operations if business systems such as billing were offline?
Check Security Team's Work	▸ Use a 3rd party to test the security of your systems and your ability to defend against a sophisticated attack ▸ Many ransomware criminals are aggressive and sophisticated and will find the equivalent of unlocked doors
Segment Your Networks	▸ It's critically important that your corporate business functions and manufacturing/production operations are separated and that you carefully filter and limit internet access to operational networks ▸ Identify links between these networks and develop workarounds or manual controls to ensure you can continue operating if your corporate network is compromised ▸ Regularly test contingency plans such as manual controls so critical functions work during a cyber-incident
Additional Considerations	▸ In addition to the White House recommendations, also consider: – Identifying high-risk employees, such as those with administrative rights to systems, who might be vulnerable to an attack or help perpetrate an insider attack – Assessing the cybersecurity programs and protocols for your key vendors — particularly any entity that handles sensitive or critical company data

Executive Order on Cybersecurity and Software Supply Chains

On May 12, 2021, President Biden signed the Executive Order on Improving the Nation's Cybersecurity (the Executive Order), which outlines a series of cybersecurity measures, including on software supply chain security, that the U.S. government will implement and become binding within approximately one year and directly impact U.S. government contractors and indirectly impact the private sector


THE WHITE HOUSE

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

Enhanced Security Requirements for Software Used by the U.S. Government and Software Supply Chains	▶ By November 8, 2021, the National Institute of Standards and Technology (NIST) will publish preliminary guidelines for enhancing supply chain security for software used by the U.S. government and by February 6, 2022 NIST will publish guidance identifying such practices ▶ By March 8, 2022, the Office of Management and Budget (OMB) will ensure the U.S. government begins implementing these requirements ▶ These requirements will discuss developing trusted environments, using automated tools and encryption methods and providing transparency to the U.S. government and other end users
Heightened Protections for "Critical Software" Used by the U.S. Government	▶ There will be additional controls and security measures required for "critical software," which by June 26, 2021 will be defined by the U.S. Department of Commerce ▶ The Cybersecurity and Infrastructure Agency will identify critical software currently in use by the U.S. government
New Standards for U.S. Government Vendors to Test Source Code	▶ NIST will publish guidelines recommending minimum standards for U.S. government vendors to test their software source code. This will include identifying manual and automated testing such as code review tools, static and dynamic analysis, software composition tools, and penetration testing
New Contract Requirements for Security Standards and Cyber Event Disclosure	▶ Within one year, U.S. government agencies will begin requiring contracts with language requiring vendors to attest to the software security requirements ▶ There will also be language requiring U.S. government contractors and vendors to collect, preserve, and share with the government data and information for cybersecurity event prevention, detection, response, and investigations

Takeaways and Impacts of the Cybersecurity Executive Order

Takeaways

The U.S. government intends to use its purchasing power to drive security standards in the commercial marketplace

- **Influencing the Private Sector**: Though this effort is directed at the federal government and its contractors, the intent of the Executive Order is to use this important market as a lever "to drive the market to build security into all software"
- **Elevating Cyber Incident Monitoring and Response**: The Executive Order outlines a series of measures, including enabling a government-wide endpoint detection system to actively monitor for malicious cyber activity on federal networks, and creating a standardized playbook for responding to cyber incidents
- **Scrutinizing Supply Chains Involving China and Russia**: Given recent cyber attacks, software development involving China and Russia likely will be subject to increased U.S. government scrutiny

Impacts

Software developers and vendors likely will need to upgrade security or potentially face adverse market impacts

- **Receiving a Consumer Rating Label**: NIST will be identifying "Internet-of-Things" ("IoT") cybersecurity criteria and secure software development practices to grade software developers on their security practices, comparable to an "Energy Star" rating
- **Attesting to Compliance Benchmarks**: Suppliers of software available for purchase by U.S. government agencies will have to attest to complying with software security requirements or have their products removed, rendering lax products obsolete
- **Cooperating with the Cyber Safety Review Board**: The U.S. Department of Homeland Security is creating a Cyber Safety Review Board to convene after a "significant cyber incident" and provide recommendations on remediation measures, generating negative publicity for software found to be implicated in such a breach