2016 CLM Annual Conference
April 6-8, 2016
Orlando, FL

"CYBER-ATTACK PREPAREDNESS TOOLBOX"

I. Introduction. The subject of a 2015 legal opinion concerning liability following a cyber-breach involved a legal action filed by the Federal Trade Commission ("FTC") against Wyndham Worldwide Corporation, contending that the company and its subsidiaries violated the Federal Trade Commission Act by engaging in unfair and deceptive trade practices. *F.T.C. v. Wyndham Worldwide Corp.*, 10 F.Supp.3d 602 (3d Cir. 2015). In this case, hackers stole, from Wyndham, personal and financial information for hundreds of thousands of its customers, which resulted in $10.6 million in fraudulent charges. The FTC then sued Wyndham in federal court, charging it with unfair business practices and contending that its privacy policy deceived customers. According to the FTC, the defendants failed to maintain reasonable and appropriate data security to protect the sensitive personal information of consumers. In support of its complaint, the FTC leveled specific allegations against Wyndham including that it (1) allowed the use of passwords that were easy to guess, (2) utilized an insufficient firewall as well as an out of date operating system, (3) failed to limit the access of third party vendors to servers and networks, and (4) failed to adhere to appropriate incident response procedures. The FTC also alleged that Wyndham failed to act consistently with its privacy policy. The legal opinion explains that a company has acted unreasonably when it fails to "make good" on the promises stated in a security privacy policy, or fails to develop and maintain an adequate cybersecurity program.

In its 2015 opinion, the Third Circuit denied the defendants' motion to dismiss, and held that an Organization can be subject to legal liability for unfair business competition if that Organization fails to maintain reasonable and appropriate data security. The *Wyndham* case is a sobering reminder of the potential legal liability that an Organization can face following a cyber-breach. For an Organization to prepare and ready itself, to limit its exposure to a cyber-breach event, in applying the *Wyndham* case, there are several steps that an Organization can – and should – take before a breach and/or a government violation occurs. These steps are discussed, below.

A. What is a cyber-breach and how do they occur? When evaluating the potential for a cyber-breach, an Organization must first determine where it stores sensitive, confidential, or regulated data (such as personal-identifying information or protected-health information). An Organization should conduct a formal audit to

determine all the locations of this data, and whether sensitive data is stored in a secure manner [note: sometimes employees keep separate files]. The key area of inquiry, when evaluating where and how data is stored, is to identify the business need for data that is collected and preserved. An Organization should not collect and preserve data that is unnecessary for its business operations.

1. **Explain what constitutes a cyber-event.** A cyber-event or cyber-breach is the unauthorized access to or use of information that is received, maintained, created or transmitted electronically by an Organization.

2. **Discuss main causes of a cyber-event.** A cyber-breach can occur in numerous ways: intentionally, by a hacker (use of malware, spyware, hacking, etc.); due to an error by an employee or business partner; or via the conduct of a malicious insider. Approximately one-third of cyber-events are caused by criminal hackers, and approximately 60% of cyber-events are caused by either employee error or a lost or stolen personal electronic device.

B. **Why must companies care about cyber-risk?** An Organization must properly manage cyber-risk. Otherwise, that Organization faces the possibility of regulatory action, as well as lawsuits including class-action lawsuits or shareholder derivative lawsuits. The failure to properly manage the risk of a cyber-attack can have serious legal implications for any Organization.

1. **Economic costs.** The economic costs of a data breach include legal costs, the retention of IT forensics experts to contain and stop a breach, regulatory fines and penalties, as well as lost business.

2. **Non-economic costs.** The non-economic costs of a data breach include damage to an Organization's brand and reputation in the business community, the loss of trust by business partners, the loss of trust by employees and customers, as well as significant interruption of business.

3. **Legal and regulatory liability.** An Organization that is victimized by a cyber-attack may be subject to liability by a regulatory body. That Organization may also find itself as a defendant in a lawsuit, including possible class-action litigation or shareholder derivative claims, depending upon the nature of the attack as well as the Organization's business.

II. **Cost-effective Management of Cyber-Risk.** The specific legal standard for cyber-risk management remains undefined. However, industry best practices indicate that an Organization should address several areas in order to properly manage this risk. An

Organization that fails to address these areas may expose itself to legal liability in the event of a breach.

A. **Management of employees**. An Organization should engage in numerous activities that are designed towards creating a "culture of cyber awareness" within the Organization.

1. **The Chief Information Security Officer.** An Organization should designate an employee who is the Chief Information Security Officer, or "CISO," and who is responsible for managing and coordinating all activities concerning the management of cyber-risk as well as securing an Organization's data. The areas that a CISO is responsible for addressing include compliance with relevant policies; drafting and enforcing information security policies; risk management including employee training and ensuring the implementation of technology safeguards; communicating with management regarding cyber-risk issues; ensuring that any necessary improvements are implemented; evaluating business partners and vendors to ensure that they are properly managing cyber-risk; and managing incident response activities

2. **Employee training.** An Organization must ensure that all employees – including executives – are properly trained on how to identify a potential cyber-event, what activities can lead to a cyber-attack, and what steps an employee can take to minimize the risk of a cyber-attack.

3. **Employment policies.** One critical area for an Organization is to develop policies regarding data management. An Organization should utilize security access controls that ensure only authorized employees have access to sensitive business data. The Organization should provide an employee with access to only that data which is necessary for the performance of his or her job, and should limit the number of employees who have broad access to sensitive business data; moreover, providing an employee such access is prudent and necessary only when there is a reasonable business purpose. An Organization that restricts access to data will help it to contain and monitor the flow of data, thereby limiting opportunities for hackers, and will demonstrate that it has undertaken efforts to maintain security.

An Organization must require its employees to use passwords that are sufficiently strong. Employees with administrative access should not use the same password for all applications, and more complex passwords should be used to protect sensitive data.

Employees must use complex and unique passwords (at least eight characters, including upper and lower-case characters and numeric and special characters), and passwords should be changed at least on a quarterly basis. Employees who regularly access data that is sensitive should be required to use two-factor authentication. Finally, an Organization's system should disable or suspend a user's credentials after a few unsuccessful attempts to log in.

An Organization should develop a plan for the destruction of data after it is no longer needed in accordance with government regulations and prudent business practices. The policy should identify the data, and discuss the process and method for identifying when sensitive information is not needed and the procedure for how such data will be disposed.

4. **C-suite and executive involvement.** Best practices also indicate that an Organization's executives and management must be apprised of the nature and extent of an Organization's cyber-risk and meaningfully participate in the management of such risk. The lack of involvement of the appropriate executives and management can lead to the termination of such employees, and exposes an Organization to potential legal liability in the event of a lawsuit following a cyber-breach.

B. Evaluation of insurance coverage. An Organization must also evaluate the extent of its insurance coverage to ensure that it has sufficient coverage in place.

1. **Evaluate the type of insurance coverage/policy language.** For example, an Organization should evaluate how its cyber-policies define "claim" or "occurrence". Often, a cyber policy will have a deductible. If each separate wrongful act or claimant or instance of data breach is a separate occurrence or claim, the deductible could devour the coverage. The policyholder must have a limit on the application of deductibles. It is also important for an Organization to evaluate whether the insurance policy provides coverage in the event that a vendor, subcontractor, cloud provider or business partner causes a data breach with that Organization's data. An Organization should evaluate whether or not its policy provides coverage for government investigations, responses to subpoenas, proceedings, inquiries and other forms of actions, whether punitive or not, by government agencies and/or law enforcement agencies. An Organization should also evaluate whether its insurance policy excludes fines or penalties that are imposed by governmental or regulatory agencies. An Organization should closely review how the policy defines such terms. For example, the coverage for

"damages" may not include "criminal, civil, administrative, or regulatory relief, fines or penalties."

2. **Evaluate the amount of insurance coverage.** An Organization should evaluate what policy limits it needs and the deductible that it is able to bear. Often, Organizations believe that cyber insurance will only be necessary in the event of a catastrophic event, and use large deductibles. Other Organizations view the risk of a cyber-event as controllable, and will use a small deductible. It is also important for an Organization to understand the relevant exclusions in order to ensure that it is covered for the type of events that are reasonably likely to occur. An Organization should evaluate its cyber-risk coverage at least twice a year, if not more frequently. Regular evaluation of such policies is a prudent practice to ensure that an Organization has protection that is current.

C. Management of business partners/vendors. An Organization must properly manage and audit a vendor or business partner who gains access to sensitive business data. The governing legal contract must include certain language that will protect the Organization, and it is important that an Organization retain the right to audit its vendor or business partners' security practices.

1. **Define who is in control of data and when.** If an Organization is going to share, with a business partner or vendor, access to sensitive data, the governing contract should clearly define who is in control of sensitive data and when. The entity that is in control of data at the time of a data breach may be subject to primary liability in the event of a data breach, depending on the nature of the circumstances that led to the breach.

2. **Protect business interests with contract language: indemnification, insurance requirements, right to audit, etc.** An Organization should ensure that its contracts with a business partner who has access to sensitive data includes appropriate indemnification language as well as insurance requirements, and reserves the right to audit the business partner's cyber-security practices.

D. **Development of emergency response plan.** An Organization should prepare and practice an emergency response plan that will be used in the event of a cyber-breach. The plan must identify the relevant stakeholders (including the immediate involvement of the appropriate business executives, legal counsel, and relevant information technology ("IT") or forensics support). The plan must also identify who will direct the response team, and describe the roles of each representative.

The failure to develop and update an appropriate emergency response plan could potentially lead to legal liability.

1. **Identify breach team.** The emergency response plan must identify the specific team members by name, and the contact information for each individual must be included, as well. The members of the breach team will include the CISO, IT personnel, other appropriate company personnel, outside vendors such as IT forensics experts, legal counsel, and others.

2. **Develop the plan.** An Organization should outline the specific steps that will be followed in the event of a data breach including which team member is responsible for handling each step.

3. **Regularly update and practice the plan.** Once an Organization develops and implements an emergency response plan, best practices indicate that the Organization must regularly audit and update that plan, as necessary. The audit process is critical in order to ensure that an Organization maintains a state of "cyber-readiness" and remains in compliance with what may become the legal standard of care. Attached as Appendix A is a checklist of areas that an Organization should address during the audit process, and a discussion of how often each item should be addressed.

E. IT/Security Issues.

1. **Evaluate your Organization's specific needs.** An Organization must use current anti-virus software, and must ensure that its servers and network devices are securely configured, and regularly scanned for vulnerabilities. An Organization must also protect its intranet with a properly-configured firewall. An Organization must also ensure that sensitive data is sufficiently protected when it is stored and transmitted, by using encryption tools when possible.

   An Organization must monitor its network and be on the lookout for suspicious activity through work traffic flow. For example, an Organization should monitor network logs and use an intrusion detection system. An Organization that knows how network activity is logged, where its logs are stored, and how long the logs are available will be better equipped to prevent and respond to a cyber-attack.

2. **Use of in-house IT department vs. external IT consultants.** While most Organizations have internal IT departments, best practices indicate that Organizations should also use external IT consultants. External consultants are likely better equipped to

conduct penetration testing and other system evaluation, and such consultants will prove to be a valuable member of an emergency response team in the event of a breach.

III. Emergency Response. In the event that an Organization becomes the victim of a cyber-attack, it will need to engage in an emergency response to that event. The goals of the emergency response includes stopping and containing the breach, restoring lost data and business operations, preserving evidence, and resuming business operations as soon as possible.

A. Attorney-Client Privilege. In the event of a cyber-breach, best practices indicate that an Organization should involve legal counsel as soon as possible. Legal counsel will be responsible for directing the activities of the emergency response team as well as communicating with the team members. The involvement of legal counsel may allow for the protection of the attorney-client privilege.

B. Assembly and notification of breach team. In the event of a cyber-attack, an Organization must ensure that its breach team is immediately notified of the event.

1. Role of IT Forensics Experts. An IT forensics expert should be immediately engaged in order to contain the breach, preserve necessary evidence, and direct efforts to resume business operations as soon as possible.

2. Role of legal counsel and insurance company. An Organization should immediately notify legal counsel of a cyber-attack. The involvement of legal counsel in post-breach activities may allow for the protection of the attorney-client privilege to certain activities. Further, it is critical that an Organization contact its insurance company immediately, and ensure that any third party vendors are approved by the insurance company.

3. Role of other breach team members. The Chief Information Security Officer and other company personnel will be involved in responding to a data breach, and will be responsible for communicating with employees, management, customers, and the public. Depending on the nature of the breach as well as the type of business in which an Organization is engaged, a public relations firm may be useful following a cyber-event.

C. Legal and regulatory issues.

1. Preservation of evidence. Following a breach, an Organization must preserve any and all potential evidence. In the event of regulatory or other legal action resulting from the breach, the

failure to preserve evidence could lead to legal liability for spoliation.

2. **Interaction with customers/potential plaintiffs.** Following a data breach, an Organization (or its public relations firm) will update customers regarding the status of post-breach activities, including the nature and extent of the breach. Given that these customers are potential plaintiffs, in the event of litigation, an Organization will want to develop a strategy, with its legal counsel, for all communications with its customers.

3. **Involvement of law enforcement.** Depending on the nature of a breach and the type of business in which an Organization is involved, the Organization may need to notify law enforcement. An Organization should consult with its legal counsel to determine what is required and what is appropriate.

4. **Compliance with state notification laws.** There are currently 47 different state notification laws in the United States. An Organization will have to comply with the notification laws of all states that are impacted by a data breach.

5. **Necessity of credit monitoring.** Depending on the breach at issue as well as the type of business in which an Organization is engaged, it may be necessary to engage in credit monitoring activities following a breach. An Organization should consult with its legal counsel to determine whether credit monitoring is necessary.

D. Post-breach evaluation.

1. **What are the "lessons learned" from the breach?** Once a cyber-breach occurs, an Organization is on notice that it may have deficient cyber-security. Such notice will become legally significant if an Organization fails to correct the areas in which it is deficient. Accordingly, following a cyber-attack, an Organization should closely examine the reasons why the breach occurred, towards the goal of preventing future breaches.

2. **What new policies are needed to prevent a future incident?** If appropriate, an Organization should develop and implement new policies, following a cyber-attack that are designed to avoid a repeat event. An Organization that fails to develop such policies may be considered grossly negligent or potentially subject itself to punitive damages if a similar attack were to occur in the future.

IV. Conclusion. In today's day and age, any Organization that is connected to the internet runs the risk of becoming the victim of a cyber-attack. The knowledge of this risk is pervasive throughout the United States as well as the world. Because of this, an Organization cannot credibly ignore this risk, and must take steps to properly manage it. The failure to sufficiently manage the risk of a cyber-attack can have serious legal implications for any Organization.

A. Why the risk of a cyber-event cannot be ignored. Under the law, an Organization can be subject to legal liability, including liability for unfair and deceptive trade practices, following a cyber-attack. The industry data indicates that liability can lead to tens of millions of dollars in costs and expenses for an Organization. In addition, an Organization that is breached will suffer damage to its reputation, may lose business, and – in some cases – may be forced to close. For these reasons, the risk of a cyber-attack cannot be ignored.

B. Benefits of taking action now.

1. Required by best practices. Industry best practices state that an Organization should take action immediately in order to avoid the risk of a cyber-attack. These best practices are outlined, above.

2. Saves time, money, and affords benefits to your business. Industry data indicates that an Organization that actively, and continuously, manages the risk of a cyber-attack will not only minimize the risk of an attack, but will save time and money in the event that the Organization is breached.