Cybersecurity: Responding to the Next Generation of Threats

Choate hosted a virtual discussion with Doug Domin, a Supervisory Special Agent for the FBI's Boston Cybercrime Squad, and Kevin Swindon, the Corporate VP of Global Security at Charles River Labs, on emerging cybersecurity threats. Joined by Choate partners Adam Bookbinder, Julia Hesse, and Justin Wolosz, the roundtable discussion covered a number of topics, including the range of cyber threats, steps for preventing and preparing for cybersecurity incidents, and strategies to address legal risks. Below are key takeaways from the discussion.

The Proliferation of Cybercrime as a Service

- There are targets of opportunity and targets of choice. Implementing strong security measures can prevent your organization from becoming a target of opportunity. Although it is harder to avoid becoming a target of choice (when an attacker targets your organization), you still want to make it more difficult for the attacker to succeed.
- Attackers are increasingly using hybrid ransomware attacks.
    - First, attackers take the organization's data.
    - Second, attackers encrypt the data and demand a ransom to release it.
    - If the organization has a backup and doesn't pay the ransom, then the attacker can still threaten to release the stolen data.

The Importance of Preparation

- Companies should make the shift from passive, incident-response to proactive, incident-readiness.
    - Preparedness requires combining a strong business continuity plan *with* a strong IT disaster recovery plan.
    - Everybody in the organization is part of a successful response – cyberattacks are not just an IT problem.
- Outside counsel and subject matter experts are crucial.
    - Retain third-party experts and outside counsel as part of your preparation.
    - Make sure that the experts you retain will provide all of the services you might need. Your organization might even need a specialized expert if you decide to negotiate and pay a ransom.
- The choice of whether to pay a ransom is difficult. An organization needs to have thought about the choice beforehand, and then needs to carefully consider the risks and benefits of paying.
- Important basic cybersecurity measures include 1) Use multi-factor authorization, 2) Restrict remote desktop protocol access, and 3) Train and educate all employees.

Legal Obligations

- Courts are becoming increasingly receptive to claims alleging only minimal harm (e.g., the cost of credit monitoring). New statutes are also creating private causes of action for plaintiffs to use.
- Cyber insurance is an important part of the picture, but organizations need to be sophisticated consumers of cyber insurance products.
    - Cyber insurance policies are not as broad as they used to be, and policyholders should pay attention to exclusions, limits, and specific policy language.

Litigation Risks

- Data breaches are often followed by class action lawsuits, securities fraud lawsuits based on a stock-drop following the breach, and derivative suits attempting to recover damages that a company suffered from the breach. Companies should consider these risks as part of their readiness preparation.

Risks from Third Parties

- Organizations retain primary responsibility for their data, and for the regulations that apply to that data, even if the data is held by a third-party vendor.
- Many of the causes of action that follow from a data breach will depend on whether your actions were *reasonable*.
    - When you choose third party vendors, keep in mind that it can be easier to defend your actions as reasonable if you were using an industry standard vendor.

For more information about the evolving landscape of cybercrime, please contact one of the following attorneys:

Adam Bookbinder
Partner, Government Enforcement Group
617-248-4806
abookbinder@choate.com

Julia Hesse
Partner, Healthcare Group
617-248-5006
jhesse@choate.com

Justin Wolosz
Partner, Complex Trial & Appellate Group
617-248-5221
jwolosz@choate.com