FOX ROTHSCHILD LLP

VIRTUAL PRIVACY SUMMIT

Our virtual conference featured leading privacy, data security and regulatory compliance professionals who addressed the most consequential topics affecting companies in every industry. Fox Rothschild's Privacy and Data Security attorneys have created this helpful at-a-glance guide to supplement the content covered during the summit.

Data Privacy for the COVID-19 Workplace

The pandemic presents employers with a novel set of data privacy threats and compliance challenges. Based on our interactive panel discussion, here are some key takeaways for companies seeking to mitigate these new risks and protect their data and their businesses.

Employee Privacy and Data Security Training

With a dispersed workforce, companies face new and emerging dangers. When employees work remotely, their professional and personal lives merge, creating a risk that they will accidentally share confidential information verbally, on various devices or via printed documents. In this environment, employees are distracted, often rushing to complete tasks, and may be more likely to fall victim to phishing attacks. More than ever, it is essential to train employees on how to maintain data privacy in a remote environment. Effective training teaches employees to:

- Avoid increasingly sophisticated scams by using only company-approved devices and being wary of calls received on mobile phones
- Be mindful of phone conversations conducted in non-secured spaces
- Identify phishing attacks, including new campaigns that target victims more directly
- Keep information secure, including by saving to the proper locations and maintaining a proper recordkeeping process
- Maintain data security while using virtual platforms
- Understand the dangers of printing and not securing confidential files
- Slow down to prevent data being sent to the wrong person, from or to a personal rather than a work email address or saved to an unsecure location
- Be proactive in reporting suspected incidents

Data Breach Preparation

Any company can experience a data breach, so preparation is essential.

- Designate at least one person to oversee issues that affect data security and oversee training, policies and incident response
- Understand where your data resides and create a data retention and destruction policy to ensure you are collecting the least data necessary in order to minimize the risk of the information being stolen or misused
- Create and enforce policies to prevent the loss of data and thwart scams such as wire/payment instruction change processes
- Purchase cyber liability coverage
- Use technology including multi-factor authentication, data loss prevention tools and link sniffing and spam/scam/phishing detection tools to protect workers and data
- Conduct a security risk assessment
- Develop a data incident response plan that includes a pandemic management plan
- Conduct a tabletop exercise to make sure you have the right data incident response plan and team in place

- Understand which policies affect which type of incident (privacy, cyber, sick with COVID in office) and make sure policies are up to date
- Update policies to reflect new issues that arise with a remote workforce and have a secure mechanism in place to report incidents
- Have a third-party call center with a script to answer questions related to the breach
- If you have a breach, work with a law firm that knows your company and is familiar with your privacy and security policies

Protecting Workers When They Return to the Office

- Develop a cross-functional team to create a return-to-work plan that protects employees in the office, specifying mask-wearing requirements, traffic flow and elevator, kitchen and bathroom use guidelines
- Have plans in place for employees to identify the location where they are working/residing (potential new applicability of state laws related to identifiable information collected by the company)
- Impose travel restrictions and ask employees to report contact with COVID-positive people outside the workplace
- Understand privacy related to health information — what is and what is not protected by HIPAA
- Protect data collected and stored related to health monitoring, including taking temperatures — ensure the data being collected is appropriate and understand what privacy laws apply to the data
- Develop reporting procedures for employees who have possible COVID-19 exposure

CCPA Is in Full Effect – Why Should You Care?

The California Consumer Privacy Act (CCPA) has been in effect since January and enforceable since July. The panel discussed a range of topics from its practical effect on businesses to what have been their biggest challenges and what businesses can expect in the future.

Key Challenges

- Companies not subject to the European Union’s General Data Protection Regulation (GDPR) experienced for the first time the significant education and preparation needed to prepare for compliance with a comprehensive privacy law and embed the understanding that “personal information” is a broad concept.
- Those already subject to GDPR worked to embed the required shift in mindset into the company culture.

Preparation

- Secure buy-in from key stakeholders by embracing privacy as a marketing strategy — understanding customers’ expectations regarding prioritizing data privacy.
- Appoint privacy “champions” or “ambassadors” to keep privacy top of mind throughout the organization.
- Engage in constant dialogue with members of various groups who make decisions regarding data so they stay up to date on the privacy landscape and view their projects through a privacy lens.

Third Party and Service Provider Relationships

- Start conversations as early as possible to determine how to handle requests for information. Start with providers that are critical to your business.
- Facts need to support classifying a vendor as a service provider or a third party. Just because you call them that in the agreement, doesn’t make it so.

Looking Ahead

- Prioritize CCPA but keep track of the changing privacy landscape so stakeholders are prepared for what privacy will look like in the future.
- Preparation and communication are key to avoid a scramble when new privacy laws are passed.
- If you are able to think ahead, focus on data minimization and record retention — time-consuming tasks that require a long lead time to implement.

Locking it Down: Preventing Costly Data Breaches and Ransomware Attacks

The COVID-19 pandemic has only emboldened hackers. Businesses face increasingly complex cybersecurity risks as they struggle to manage fully or partially remote workforces. Our panel explored emerging cybersecurity issues, the increasing threat from ransomware and offered actionable advice on how businesses can protect themselves.

Ransomware – the Change in Data Theft Behavior

- Frequency and severity of attacks has increased during COVID. This is partially attributable to remote working — employees are less diligent and more distracted.
- More sophisticated threat actors are focused on gathering data that will help them know their victims. In addition, they are focused on:

  o Using phishing emails to download sophisticated malware

  o Taking advantage of unsecured desktop applications to access information

  o Identifying increased VPN vulnerabilities

  o Finding an open port, getting a foothold, landing and expanding to identify the company's financial system and backup system — whatever is needed to force a ransom payment.
- More effective attacks have resulted in an increase in ransomware demands. Even the most basic ransomware attack is expensive. In the second quarter of 2020, the average ransom payment was $178,254 — a 60% increase from the average in the first quarter.
- While initial ransom demands increased dramatically, actors are willing to negotiate to obtain a payout. However, they use time pressure against the victim to extract payment quickly.
- There is a huge payoff for cyber threat actors. The attacks would not continue if businesses were not paying the ransoms; however, many are paying due to the potential reputational harm if they fail to pay.
- It is anticipated that the attacks will subside as there is significant administrative work and cost involved for cybercriminals in keeping targets' data sets separate. Some have begun to send the wrong data sets to victims, indicating that they can't keep up the pace.

Common Data Breach or Ransomware Attack Costs

- A ransom payment is a hard cost. However, a ransomware attack can put a company out of business, and this often has little to do with the payment itself.
- Other common costs associated with a ransomware attack include:

  o Restoring systems

  o Rebuilding data

  o Forensic investigation

  o Legal and coaching costs

  o Credit monitoring and dark web monitoring if personal information was exposed

  o Regulatory investigations and fines

  o Lawsuits and/or class action claims

  o Business interruption cost, which increases the longer the company is down as a result of the attack

  o The need, in some cases, to build a parallel network so it cannot be reinfected

Ways to Prepare for and Avoid Data Incidents

- Employee training
- Multifactor authentication
- Partner with your cyber insurer to help with risk mitigation — the insurer can help identify vulnerabilities based on external facing infrastructure
- Conduct a data governance initiative to better protect and store the most important information and identify the data the business truly needs to save
- Develop an incident response plan so the company has the right team and plan in place to respond to an incident