Published on *The National Law Review* https://natlawreview.com

The FTC Gives $3M Reasons To Ramp Up Cybersecurity

Article By:

IMS Legal Strategies

How much should you invest in cybersecurity this year? While the question is relative to your company's size, services, and needs, does knowing the FTC is investing nearly $3M make you reconsider?

In the wake of the recent data breaches, the government is taking measures to ramp up its e-discovery capabilities and data security detection technology. Why? Because if consumers are purchasing, ordering, renewing, and refunding almost exclusively online then the consumer protection battlefront starts with the internet. If the FTC is gearing up for an unprecedented year of cybersecurity investigations and litigation, shouldn't you?

In a very exceptional move, the FTC awarded a nearly $3M litigation support service contract to Innovative Discovery, LLC of Arlington, Virginia without collecting competitive bids. With the rise of companies in the last ten years having built online platforms to initiate consumer interaction, obtain the necessary identification information, and facilitate purchasing strictly via the internet, more breaches are expected to occur.

Measures to Take

In order to ensure cybersecurity and deter companies from collecting personal consumer data by fraudulent means, as well as motivate companies to take proactive measures to reinforce data security in a growing digital world, the FTC is rightfully gearing up and so should you. Here are a few tips from cybersecurity experts on some more affordable measures you and your clients can take to help improve internal data security in the coming year and your likelihood that an Equifax-like breach and subsequent government investigation doesn't happen to you:

- **Strong Password Policies**: While this may sound overly-simplistic, the fact remains that the best way for a hacker to infiltrate the system and gain more access to secure files is to enter via an employee's password. Initiate a policy for mandatory, company-wide change of passwords by the staff at least once each quarter. Advise employees not to save passwords on a computer file but, rather, in handwritten form stowed somewhere safe. Send a company-wide email once a quarter reminding staff members to do this and confirm compliance. Remind employees common names (spouses, children, pets) and dates (anniversaries, birthdays) can often be guessed rather easily from a quick browse of their social media

pages. Simple, internal (and more affordable) measures like this can go a long way.

- **Internal Cybersecurity Training**: If a hacker cannot ascertain an employee's log-in credentials by guessing, the next best way is to ask for them in a seemingly benign, protected mechanism—*i.e.,* an email or pop-up screen perhaps. If staff members are trained on how to spot common hacking mechanisms designed to elicit log-in credentials, this will increase the likelihood they will not inadvertently provide hackers access to the system

- **Penetration Testing:** Penetration testing by a cybersecurity expert is an excellent way to detect vulnerabilities in your system and proactively protect against threats. These tests challenge your existing security systems and expose weaknesses by trying to bypass them through commonly-utilized hacking techniques. While any implementation of expert services and testing will come with a cost, it can be well worth the price to avoid a far more expensive data breach, protracted litigation, and loss of good will after public disclosure. In addition, proactive attempts to uncover and correct potential problems *before* they lead to security hacks can go a long way to show compliance with industry regulations if you do find yourself under investigation by the FTC.

- **Ethical Hacking:** Here, cybersecurity experts simulate a real attack by mimicking techniques used by criminal hackers to infiltrate your system. Going one step beyond penetration testing, which involves bypassing firewalls and predicting passwords, ethical hacking can employ more aggressive techniques such as phishing attempts and more. This type of isolated hacking will not only test your systems but your staff as well.

The vulnerability of your customer and client data is, unfortunately, a necessary evil in today's ever-increasingly digital world. If you or your clients are looking to bring in a cybersecurity expert to help test and improve your data security systems, we know just where to look. The FTC is gearing up for 2018, and so should you.

National Law Review, Volume VII, Number 312