TX Office: (817) 416-6842
NV Office: (702) 565-2727

Kral Ussery
Certified Public Accountants
Advisors - Litigation Support - Internal Audit

**March 24, 2022**

# Cybersecurity Tips for Recovering From a Cyber Attack

Try as you might, cyberattacks are impossible to completely prevent. Wealth and asset management firms perform large financial transactions and harbor even larger volumes of sensitive client data and intellectual property, making them uniquely vulnerable to cyberattack. A recent survey reveals that the average financial services firm is the target of 85 data breaches per year. Common as they are, a breach can have devastating consequences for your company. In addition to information and finances lost, breaches can result in downtime and reputational damage that can set your firm far behind competitors. The following tips can help you make it through a data breach and come out stronger than before.

### 1. Keep calm and carry on

You just discovered you've been hacked. First order of business? Don't panic. Next, go off the grid. Hackers use your system's interconnectivity to escalate attacks, winding their way through devices and data sets in search of valuable information. Disconnect from the Internet and change all passwords — even the ones that grant access to unaffected sites and services. You may have the urge to delete data, but don't give in. Not only are you deleting data that might be salvageable, but you're also deleting the evidence you'll need to report the breach to your cyber liability insurance carrier, or depending on the type of data compromised, law enforcement. Inform your incident response team that there's been a breach and open an investigation into the hackers' motives. Identify which data they're after and why.

A growing number of hackers are after a ransom. In the first half of 2021, ransomware increased by 93% compared to the same time period in 2020. Ransomware attacks are increasing in frequency and they're becoming more costly. The first quarter of 2021 saw the average ransom rise 43% from the previous quarter. If ransom is their motive, hackers will let you know. If it seems that they're stealing data, they probably plan to sell it or cause you reputational risk. In late 2020, several unlucky asset and wealth management companies discovered their confidential information on public data leak sites. Once you have an idea of your attackers' motivation, you can weigh your options as to how to respond. At this point, your incident response team should be working to remove hackers from the system.

### 2. Communicate effectively

Data breaches often have a ripple effect, impacting everyone from management, to clients, to vendors, to stakeholders. Transparent communications with all involved play a key role in helping firms regain trust after a data breach. Once the threat has been successfully neutralized, you must deal with the fallout. Notify staff that there's been a breach and outline any actions they can take to minimize the effects. If client data was compromised, let clients know. Be sure to disclose relevant details and clarify the steps you're taking to rectify the situation. After clients have been informed of the breach, it's time to tell investors and other stakeholders. If you have cyber liability insurance (and you should), contact your carrier as soon as you can. Present them with a

detailed timeline of events as well as any evidence you've gathered throughout the attack and ensuing internal investigation. Your carrier will advise you on next steps and put you on the path toward financial recovery.

**3. Ask "why me?"**

In many cases, hackers infiltrate a company's system weeks to months before they ever launch an attack. They use this time to observe operations and identify opportunities to strike. Once the dust of a data breach settles, it's imperative that you assess which factors made you vulnerable to attack as well as the efficacy of your incident response.

Use this period of reflection to strengthen your defenses. Install the latest cyber security controls and reexamine the security of interactions with collaborators, vendors and business partners. Perform due diligence and revise contracts to ensure that existing and future relationships are in the best interest of your firm and your clients. If your incident response team was not as helpful as you'd hoped, it might be time to revise your incident response plan and train IT personnel in your improved methods. Cybersecurity efforts are commonly undermined by the pervasive misconception that bolstering cybersecurity is an expensive undertaking. The truth is it is far more cost-effective to invest in cybersecurity now than recover from a future cyber incident.

**Consider it a lesson learned**

Cybersecurity goes well beyond preparedness. Despite your preventative efforts, your wealth and asset management firm can be targeted in a cyberattack. To mitigate the damage, it's critical to arm your organization with an Incident Response Plan before the attack occurs as time is of the essence for swift recovery. This plan should be tested periodically. Enhance controls designed to help disarm the hackers, uncover their motivations, be upfront with all affected and take it as a lesson in the importance of a holistic approach to cybersecurity.



*****

**Kral Ussery LLC** serves US public and private companies to protect and grow shareholder value, as well as non-profits and governments with internal controls and in combating fraud. We assist entities in all matters relating to financial reporting, including SEC compliance, internal controls, SOX-404, IT general controls, IPO & SPAC readiness, M&A transactions, US GAAP compliance, and cybersecurity readiness. Visit us at www.KralUssery.com.

**This is an article from the Governance Issues™ Newsletter, Volume 2022, Number 1, published on March 24, 2022, by Kral Ussery LLC.**