BREACH RESPONSE CHECKLIST

News of a cyber breach is certainly news nobody wants to hear. But cyber-criminals seemingly never rest, and here's what you'll need to do in the event hackers find their way in:

☐ 1 ENGAGE YOUR EXTERNAL PARTNERS

Your cybersecurity and compliance partners will play a critical role following any data incident. This includes assessing what data or systems were compromised, restoring systems to full functionality, and dealing with the proper regulatory bodies for compliance and reporting purposes. Working with your partners as soon as possible after a breach will allow them to deploy their expertise to limit the damage and prevent future incidents. In order to effectively respond to a breach, partners from cloud storage providers to penetration testers need to all be focused on giving you all the assistance you need.

☐ 2 NOTIFY YOUR CUSTOMER BASE

There are numerous cybersecurity regulations that likely require you to report the incident to customers or clients whose data may have potentially been compromised. If, when, and how you'll need to do this will depend on factors like what industry you're in, the type of attack you've suffered, and what kind of information hackers may have gotten their hands on. Once you've worked with the proper agencies - alongside your cybersecurity partner - contact the appropriate customers letting them know what happened and the actions you're currently taking to prevent future ones. If you have a public relations crisis management team, now is the time to loop them in. Your crisis management team will help control internal and external messaging, and their communications to your customers and the public should be clear, concise, and consistent.

☐ 3 INITIATE YOUR RESPONSE PLAN

Every business that handles sensitive data should have a cyber-incident response plan in place. As soon as the breach is identified, begin execution of your response plan by assembling your pre-determined incident response team. This typically includes an incident response leader, along with point people from departments like management, information technology (IT), human resources, and public relations. Keep in mind that while executing your response plan, the data incident may compromise intra-organizational communications. Have contingencies in place for such an event, including having laptops ready that aren't connected to the network.

☐ **CYBER INSURANCE** Keep your business on a stable financial foundation should a cyber security event occur - get cyber damage and recovery insurance today.

RSI Security | 858.280.3330 | info@rsisecurity.com | rsisecurity.com | San Diego, California

BREACH RESPONSE CHECKLIST CONTINUTED...

☐ 4 INVESTIGATE THE INCIDENT

Aside from simply wanting to know what went wrong, regulatory bodies will likely require you to conduct a thorough investigation into the breach. You'll want to make sure all relevant stakeholders are involved in the investigation, and carefully document your findings for reporting purposes. One member of your incident response team should be charged with identifying and collecting information about the incident. This includes interviewing involved personnel and forensic documentation such as what data was viewed/modified, what information was compromised, and measures necessary for system restoration.

☐ 5 REPORT TO AUTHORITIES AND AGENCIES

Work with your internal compliance team, third-party cybersecurity partners, and any outside legal counsel you may have retained to come up with a game plan for compliance reporting. As of 2018, all 50 states in the U.S. have standing breach notification laws, and certain states require that you automatically notify law enforcement in the event of a breach. Also review relevant company agreements, like website privacy policies, that may have been impacted and require notification of regulators and/or your customer base. Breaches may affect customers in different states - with varying regulations - so make sure each relevant agency is contacted and cooperated with fully.

☐ 6 INCIDENT ASSESSMENT AND PREVENTION

Once you've worked with your response team and cybersecurity partner to quarantine and eliminate the threat, you'll want to conduct a thorough assessment. You'll want to look for ways to mitigate future risks by determining if there are any adjacent security gaps or risks, or if any other systems might be under immediate danger of a similar attack. Address any weaknesses in your system infrastructure, data handling policies, and your incident response plan. You may also want to conduct security policy review training to ensure that your employees aren't the weak link.