Steps To Follow After A Data Breach

At some point, every organization will have to deal with some sort of cyber incident. In a perfect world, the post-attack reaction is well choreographed, with everyone taking their positions and flawlessly executing their often-rehearsed roles in the data breach response plan. More often, incident response resembles a group of young children on a soccer field. It's pure chaos, with everyone surrounding the goal and trying to kick the ball at the same time — no one has any success. It might look cute on a schoolyard, but that type of reaction by the security team will lead to large fines, loss of business and reputation, and in some cases, employees being fired. The attack itself is inevitable; 62% of companies dealt with a cyber incident or data breach in 2021, according to a KPMG survey. So, it isn't the incident itself that will be the biggest problem. How an organization reacts in the aftermath and how they come out on the other end will make all the difference.

Communication

Long before a data breach, well-prepared companies will have their incident response team in place, including representatives from the security and IT teams, legal, marketing and public relations, maybe human resources. Hopefully, this group will conduct tabletop exercises with enough frequency that all the players know exactly what to do so the reactions are instinctive, not panicked. The technical response to a breach is important, of course, but perhaps the most vital action from the response team is its communication. How a crisis team works together depends on how well it communicates. There will be several legal issues around what you can and cannot say. What happens too often is people will overshare information about the breach. Oversharing too early in the mitigation process leads to speculation because the details of the incident aren't complete. Putting out incorrect or misleading information creates new layers of damage. The communication strategy is layered. It begins internally, among the incident response team and then through the entire company, and moves externally, to customers, third-party contractors and the media.

Agility, Flexibility, Scalability

Putting the data breach response into action requires agility, flexibility and scalability. The incident playbook will provide the guardrails, but there has to be a willingness to react and scale up to the realities of what could happen in the next hour, next day and next month following a breach. There is a lot of uncertainty around a data breach about the best way to keep the business running or whether to pay a ransom. Those decisions can't be made until the impact of the incident is fully known. Many companies do not have incident response plans—and for those that do, when the incident happens, does the plan get used? Too often, the answer is no.

Well Handled Or Fumbling The Response

Uncertainty makes itself known in the response team's communication style. The team's first decision is two-fold: Who should a business notify first, and at what point in the remediation process does the notification occur? If you go out too soon and provide only vague details, that's not going to inspire a lot of confidence. At the same time, you won't ever have full details to report. Once the incident is announced, the questions will come flooding in from all directions, and the way the organization responds to this will seal the perception. Managing the incoming is the thing that I think most makes or breaks

the response to a cyber incident, because if you do it well, people say, ‘okay, you’re on top of it, I trust you.’ If you don’t do it well, they say, ‘oh well, they’re fumbling. They can’t answer my question, so they probably don’t know what they’re doing.’

Follow A Checklist

In the aftermath of one of the more infamous cyber incidents, the cyberattack on SolarWinds, the company didn’t trust their email system for a period of time during the aftermath. This left their employees without an internal communications system and no easy way to stay updated, according to Pam Nigro, VP of security at Medecision and ISACA board chair, and Rob Clyde, executive chair of the board of directors for White Cloud Security and ISACA board director. There was no guidance on how to keep communications flowing because no one was sure if the infrastructure was still infected with intruders, Nigro told Cybersecurity Dive. Following the playbook could have helped that, but a better solution is to augment the playbook with a checklist of things to follow as the response is playing out. ISACA created such a checklist for a ransomware response, but it can be used as a guideline for any type of cyber incident.

Look At The Cause

Once the worst of the remediation is complete — the communications have been successful and the system is deemed clean and safe — it is time to address the cause of the breach and ensure that other potential vulnerabilities aren’t hiding, waiting for the next exploit. Having the right people on the team, and bringing in the right people from outside if necessary, will be key in any incident response. That level of preparedness could be the difference between a data breach that gets handled smoothly with minimul visibility versus a catastrophic event that leads to everyone looking for a new job.