After The Data Breach

How a Company's Recovery from a Data Breach Impacts its Long-Term Viability

FORTRESS STRATEGIC COMMUNICATIONS, LLC.

LIFARS

your digital world, **secured**

Once a data breach has been identified and contained, the recovery process begins. The recovery process is just as crucial as the readiness and response stages: failure to follow the correct procedures could significantly impact the company's operating capabilities in the near and distant future. In this final of three articles, **LIFARS, LLC. and FORTRESS STRATEGIC COMMUNICATIONS, LLC.** outline steps companies need to take after they contain the data breach and initiate the process of normalizing business operations.

Data breach recovery is a complex process that requires appropriate, precise and coordinated procedures. In this final component of the data breach lifecycle there is a lot of attention paid to not only identify how the breach occurred, but also to implement appropriate remediation steps and strategies to ensure that the incident does not occur again. The steps to data breach recovery include:

1. Verify that **containment and cleansing** is complete. During and after a breach, indicators of compromise need to be created and listed. These indicators include malicious executables, file modifications, processes, system calls, network connections, and many other items. These are a set of qualities that can be used to identify compromised or infected devices. With these a post-breach cleanup becomes easier, although sometimes it may require a rebuild of critical devices such as database and application servers. In these cases, having backups can greatly reduce downtime.

2. **Business continuity** begins once the confirmation phase is complete. This ensures that the newly rebuilt environment is not re-infected. Once the environment has been secured to prevent further infections via known indicators of compromise, it can be restored before the remediation begins so that the business can begin running as normal. This phase is heavily dependent on the backup and Disaster Recovery and Business Continuity plans and steps that have been taken prior to the incident. If they were not sufficient or did not exist, notes should be made to improve those weaknesses for future incidents.

3. After cleansing the environment, the next step is to **find the weak points in the architecture** that allowed the compromise. Architectural weak points are found by identifying the methods the attacker used to breach the system. If the attack came in through unsanitized input and uploaded a remote shell, then the weak point is both the application for allowing such, and the server for not detecting an upload. Using this, gaps can be filled in many areas reducing the response time in new incidents or even preventing incidents. This may include adjusting log levels, timestamps/time-syncing, changing the IR plan, updating and patching systems, implementing or deploying security tools, and/or modifying the functionality of systems.

4. Once weak points have been patched, the next remediation step is to **test the new environment**. The testing process should include a dedicated outside team, engineering, management, and compliance. The test is carried out in a similar manner as the attack plus some additional insight by the team to find more vulnerable areas. This will ensure that the changes have not opened up another hole and were effective. This usually includes replaying the attack vector, as well as then going for a more comprehensive test. Once it has been tested the remediation is mostly complete from the technical standpoint.

5. After the breach, **compilation of new policies** must occur and be implemented based on all lessons learned during the entire lifecycle of managing the breach. These will usually help create operational standards that include topics such as updating, incident response, backups, security device usage, and the like. These policies will serve as a long-term foundation for a holistic security practice. They should be retested within six months of their initial deployment to ensure the gaps have been filled.

Crisis communications usually ends when the data breach incident is deemed over and all management, investigation, cyber security, and remediation actions are complete. Reputation protection and communication, however, never end. Once the crisis is in a manageable state, the company needs to transition back to its regular public relations and reputation management activities. An effective post-crisis phase features four key strategies:

1. **Conduct a crisis communications postmortem**. Even when a company manages crisis communications effectively during an event, some aspect of the communications process almost always emerges that calls for improvement.

This postmortem process discovers and describes areas for improvement in crisis communications. Rich in detail, it involves input from a wide array of role players including the crisis communications and management team, the company C-suite, key employees, vendors, and partners. Key journalists the company has established relationships with can add valuable input. Customers and clients can also be surveyed via a variety of methods. Media coverage and social media comments should be collected and analyzed. The objective is to determine the efficacy of the company's crisis communications: that is, what worked, what did not work, what should be kept the same, and what needs to be changed. Once all results are in, they should be analyzed and incorporated into a report for dissemination to all relevant parties.

Most importantly, the company crisis communications and management plans should be revised based on the findings of the postmortem. In addition, the plans need to be tested to ensure that they work and deliver the necessary results.

2. **Provide the necessary support**. Just because the crisis is deemed over, that does not mean the company's responsibilities to those impacted are over as well. If customers have had information stolen, need identity theft protection or counseling, etc., the company must do everything it can to ensure that all impacted parties feel that they are being looked after. In some cases, this support may need to last for an extended period of time. Ultimately, the company should not look at support as a burden or expense; rather, it is an investment in their reputation and customer loyalty. Customers expect that the company will help them through a crisis, and a solid response increases the likelihood that customers will spread the news that the company takes good care of its own. The power of the spoken word, coupled with positive social media commentary, can deliver significant reputational benefits.

3. **Continue to communicate**. Similarly, just because the crisis is declared over, that does not mean the company should stop communicating about the crisis with all affected parties, i.e. the media, employees, and customers. If customers were directly or indirectly impacted by the breach in any way, proactive company communication must continue for the duration of the remedial action--and beyond. Messaging needs to be amended accordingly. Customers want to know that the company is still looking after them and they want to know specific steps the company is taking in response to the incident.

Some companies may choose to share a case study of how the crisis was handled with key business and trade media. This action achieves two important objectives: it demonstrates to the media and stakeholders how well the business handled the crisis, and it defines and clarifies lessons the business learned and incorporated into future plans. Regular public relations should be resumed, and the company should be prepared to deal with ongoing media questions pertaining to the crisis.

All parties will also need to be shown the measures being put in place to ensure the data breach does not happen again. Obviously, highly sensitive information must not be divulged. However, there must be some form of communication that shows that the company knows what went wrong, how it occurred, and what the company is doing to prevent the same or similar type of breach from reoccurring.

4. **Continue to monitor stakeholders**. Companies should continue to monitor media comment, customer opinion, and communications from other stakeholders. Media comment can be monitored via a media monitoring solution along with reviewing key publications on a daily basis. If any irregularities or inaccuracies are identified, the responsible publication/journalist must be contacted and persuaded to issue immediate corrections and amendments. In addition, customer sentiment can be monitored in the social media universe and in call

centers. Any inaccuracies, discrepancies, and incorrect perceptions need to be addressed quickly and appropriately. Stakeholders such as shareholders, investors, and employees should be contacted for insight and listened to carefully so the company has an enterprise-wide understanding of the perception challenges it may be facing.

Managing a data breach must be seen as more than simply having a plan to "deal with things when they arise." Data breach management is an integrated process that consists of three distinct phases, all with their own appropriate and flexible plans of actions and messaging. A company that is prepared for a data breach will have a significant upper hand in the management of the crisis and in the highly sensitive communication during the crisis. Their ability to respond intelligently and responsibly will ultimately impact their reputation and the perception of their company, its brand, reputation, and the products, goods, and services it has on offer.

In these times, it is not a case of if there is a data breach, it is a case of when. The best approach to handling a data breach is to be ready with a rapidly implementable plan of action and have well-versed external consultants available to help guide the company through the critical event.

Data breach readiness is an ongoing and never-ending reality.

FORTRESS STRATEGIC COMMUNICATIONS, LLC.

Fortress Strategic Communications provides specialized strategic public relations and crisis communications consulting to startup, medium and large companies that offer products, services, and solutions designed to manage and mitigate all types of risk. For more information please visit: www.fortresscomms.com or contact us at- info@fortresscomms.com or 315 744 4912

LIFARS

your digital world, **secured**

LIFARS helps businesses defend their networks and reputation by providing elite cybersecurity solutions with military-style Incident Response and Digital Forensics. Through decades of hands-on experience with high-profile cases, we are uniquely positioned on the cybersecurity battlefield and our mission objective is clear: protecting your business. For more information please visit: www.LIFARS.com or contact us at- info@LIFARS.com or 212 222 7061