Data Breach Readiness

Incident Response and Reputation Protection Plans are the Key Components of Data Breach Management

FORTRESS STRATEGIC COMMUNICATIONS, LLC.

LIFARS

your digital world, **secured**

Many prominent American corporations endured database breaches in 2015. Unfortunately, 2016 will be no different. With cybersecurity threats on the rise, the adage of "not if, but when" holds truer than ever. Businesses of all types, including financial service companies, should take significant steps now to mitigate harm and protect their stakeholders, their reputations, and possibly their very existence. In this first of three articles, LIFARS LLC and FORTRESS STRATEGIC COMMUNICATIONS LLC look at ways companies can prepare themselves to identify, address, and recover from database breaches.

Data breach incident response plans can, if properly implemented and tested, save your business in the most critical of moments. The importance of proper preparation cannot be overstated. Managing a cybersecurity incident versus simply "surviving it" makes a major difference in the resulting impact on business. A well-structured, holistic cybersecurity incident response plan will help manage a seemingly unmanageable scenario. When dealing with privileged and confidential information, time is of the essence and being prepared always delivers superior results.

Information Assets: The most important action in any incident response plan is to identify the so-called "crown jewels" – the most valuable data (or assets) critical to the operation of your business. Without knowing what you are protecting, it's very hard to effectively do so. Defining your crown jewels is key. Each organization has different crown jewels, but they are typically substantially similar within a given industry.

Once identified, it's necessary to become familiar with the environment – knowing precisely where on your network they are located and which users have access to them. It is also necessary to establish where "ownership" of the data assets resides. This entity will be fully responsible for the data and will be the point of contact during an incident response.

Lastly, it is necessary to establish baselines for critical data security processes and controls. This will help detect any intrusions in a timely manner and provide a solid starting point for the incident response or digital forensics investigation.

Technical handling of the data breach: Early detection is crucial for an effective cybersecurity incident response. "Time is money" and this holds especially true for data breaches and their impact on business. Advanced Persistent Threats are now common and difficult to detect. Fortunately, there are new technologies available that can speed up the meantime to detection - including advanced malware detection, from Cyphort, next-gen SIEM technology like LIFARS TIMS, and advanced endpoint protection, such as EnCase, and many others.

Detecting a breach is only part of the story; an effective incident response is equally as important. The emergency incident response team needs to respond swiftly and with striking precision. This can only be achieved if the team of responders is a dedicated internal team or a retainer-based team with a SLA-specified guaranteed response time. A retainer-based incident response team must have an in-depth knowledge of your environment and a strong connection to the internal IT teams. The responsibilities of the internal and external teams must be clearly defined prior to an incident. The external IR team has to be well informed about the persons responsible for various assets and systems within the network. As an example, the IR team must know who has the necessary privileges to the access logs. Having to search for that person at the time of a breach can take a long time and can become very costly.

Tabletop exercise: To better prepare for the various situations that might arise (i.e. DDoS, ransomware, insider data breach, etc.), it is important to conduct tabletop exercises and explore the various possible threats and ways to mitigate them. Tabletop exercises are an important tool that provides a high-level estimate of the success of handling a given cybersecurity incident situation. To ensure the best results, find the time to prepare properly for the exercise and give a lot of thought to the various options available. It's best to involve multiple departments and parties to have a more complete understanding of the emergency scenario. The legal department, in particular, is a crucial part of any data breach tabletop exercise.

Before conducting a tabletop exercise, it is important to let all of the participants know what the rules of the exercise are, otherwise some parties involved might get frustrated and not want to attend future exercises. Various industry organizations and the government provide resources and information for tabletop exercises. In most cases, organizations also benefit from having an external cybersecurity company conduct the exercise. This helps deliver objectivity and brings a new perspective and ideas to the table, along with past experiences. Lastly, the exercise should always be as wide-reaching as possible to encompass the plethora of various options available.

Test the plan: After completing the tabletop exercises, it is advised to perform a test of the incident response plan. The test could vary in scope and intensity. Some cybersecurity companies offer incident response tests by realistically simulating a cyberattack – for example by launching a spearphishing campaign followed by an attempt to breach the network and access critical data. This type of test can push the IT security team to the limits, but the results are always positive. Any gaps are revealed and the overall efficiency of the plan is tested and can be improved upon, fortifying your defenses in the process.

When developing a data breach incident response plan, decision makers need to make safeguarding the company's reputation top priority. Failing to do so could potentially lead to severe implications for their business.

Reputation protection commences long before any cybersecurity incident or crisis arises. Unfortunately, pre-crisis readiness is often either neglected altogether or approached solely from a crisis planning perspective. In fact, crisis planning is just one of several responsible steps a proactive business should implement; all elements of business planning should serve as integrated components of a larger reputational management strategy. Three key communication steps are essential to crisis readiness:

Implement an internal communications campaign: Internal communications are a core component of both strategic public relations and crisis communications. When a critical event occurs at a company and it spills over to the media, journalists often approach employees for more information. While companies need to have enforceable media policies in place that clearly delineate who can and cannot speak to the media, policies are no guarantee that employees will not talk to the media when pressured, as is seen in articles regularly attributing quotes to "someone close to the company" and "anonymous sources."

Companies should implement a robust internal communications campaign that internally delivers the same messaging that is disseminated to external stakeholders, including the media. Strong internal communications keep employees motivated and invested in the well-being of their company. Informed employees have greater trust in their employers and their company and can serve as excellent brand custodians. When they feel involved in and committed to their company, they are more likely to share factual, honest, and accurate information.

With a consistent communications framework in place, when a crisis breaks, critical messages and information can be communicated with minimal lag time and a highly reduced risk of error. Regularly informed employees have easy access to uniform messaging. As a result, when employees are contacted by journalists, they will be prepared to respond appropriately and direct the media to the company spokesperson. Even if they decide to break with company communications policy, at least they will have access to the same consistent messaging as everyone else.

Invest in a public relations campaign: Investing in public relations lays a strong foundation for a proactive communications campaign in the event of a crisis. More often than not, during a crisis, a company will communicate with its regular media, i.e. trade and various vertical media, as well as general news and investigative journalists. When a crisis breaks, journalists who have received regular company communication about new product launches, deal announcements, and bylined thought leadership articles will by default understand the company better and can write with more authority and clarity about the business. Informed journalists are less likely to make a factual error when covering a crisis. Correcting inaccuracies in news articles in the midst of a crisis can cause additional headaches that can be avoided by building solid media relationships ahead of time.

An effective public relations campaign entails more than simply sending out company news and generating a bit of social media activity. It must also include relationship building among key publications, journalists, C-suite executives, and the company spokesperson who will lead the public face of the company during a crisis. Building the critical components of trust, respectful relationships, and clear communication when business is running smoothly will help companies reap immeasurable benefits when the going gets rough.

An excellent public relations plan goes beyond media relations to include stakeholder communication via content marketing and social media communications through relevant channels and platforms. A monitoring component for print, video, and social media can serve as an early warning system to correct misconceptions before they get out of hand and address developing issues and trends as quickly as possible.

Formulate an enterprise-wide crisis communications plan: Many companies create crisis plans based on a simple template, often downloaded from the internet. However, crises do not follow templates. They occur at inconvenient times with varying levels of intensity and unpredictable twists and turns.

A vulnerability and risk audit can determine risks, threats, and anticipated impacts a business may be susceptible to. Such an audit facilitates resource planning, and, if done correctly, it can prevent the dreaded secondary crises, which often emerge out of a primary crisis.

The crisis plan should include the usual suspects: a list of crisis team members and their roles and responsibilities, contact details and a call tree, core messaging, strategies and policies, etc. The plan must designate a specific spokesperson to lead all internal and external crisis communications. The company spokesperson should be media trained and provided with a yearly refresher course. Most importantly, the crisis plan must be tested and exercised and then updated for continuous improvement.

Preparing for a data breach is fundamental to ensuring a company's vitality and sustainability. Proactive readiness helps a company respond more quickly and reduces potential reputation damage. With the ongoing news of companies and government agencies being hacked across the country, customers and partners now expect organizations to take the responsible steps of identifying where they are vulnerable and implementing the necessary plans and processes to respond accordingly. Just as when responding to a fire or a flood, time is always of the essence in a data breach, so well thought-out preparation is essential.

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

Responding to a Data Breach

How Immediate Response to a Data Breach Improves a Company's Ability to Regain Trust, Rebuild, and Thrive

FORTRESS STRATEGIC COMMUNICATIONS, LLC.

LIFARS
your digital world, **secured**

Dealing with a data breach is a complex process. In many cases, companies experiencing a breach do not know what they will find. They will have trouble assessing how much damage has been done to their infrastructure, their bottom line, their ability to continue providing services, solutions and products, and, most of all, their reputations. In this second of three articles, **LIFARS, LLC. and FORTRESS STRATEGIC COMMUNICATIONS, LLC**. look at how companies can effectively respond to database breaches.

2015 was a busy year for data breaches and Forbes Magazine[1] highlighted a few of them:

1. Anthem - 80 million patient and employee records compromised
2. Ashley Madison - 37 million client records compromised
3. Office of Personnel Management - 21-25 million federal workers records compromised
4. Experian/T-Mobile – Records of 15 million people compromised
5. Premera BlueCross BlueShield - 11.2 million subscriber records compromised
6. LastPass - 7 million users compromised
7. CareFirst BlueCross BlueShield - 1.1 million records compromised
8. Kaspersky - multiple customers affected by the compromise
9. Hacking Team - million emails compromised
10. Slack - 500,000 email addresses and other personal account data compromised

1 Issue: December 31, 2015

Data breach detection requires an immediate response. Having the appropriate steps in place with a policy, procedure, or guideline set is important and can greatly reduce time. Often, however, this isn't the case until after a breach is suffered. Additionally, having tools and trained staff is another overlooked but greatly helpful component of the breach response strategy.

1. The first step is to identify the situation. Often this means having the user step away from the keyboard and calling IT immediately. IT will then look into the issue and act as a filter before escalation. Usually it is a false positive or something minor that is not a breach, but once the severity has been determined, and the affected machines are known, then the Immediate Response Team in conjunction with an IT security team member should begin documenting everything they can, as well as saving files and collecting logs. This includes descriptions of the user and the actions they have taken, times, what is on the screen, what immediate actions were taken, and any additionally relevant information that they think is important and then escalating that to the relevant parties. Often this is just an IT manager, but it can include the security staff as well. The goal is to ensure that all immediate steps have been handled properly before moving to the organized response. The key factors that the immediate response team will look for to determine if a breach occurred include external connections that have been established to unknown destinations, data loss or corruption, apparent or suspected remote control, downloading files or suspicious objects, and any anti-virus or other alerts.

2. More often than not, incidents are outside the scope of the experience of many IT teams, even those in IT security. In many cases, companies have external technical teams placed on retainer for advice, or for immediate response to lend specialized expertise to the ground forces. It also helps companies to have the additional technically trained IT security staff who are appropriately skilled, as most IT teams are not able to handle the additional workload of a breach while simultaneously maintaining their day-to-day jobs.

3. Once a situation has been determined, the next piece is to find out who is involved in the response, both from a non-technical and technical perspective. In many cases, this will be legal and the IT security department if it exists. Sometimes, it can involve C-Level executives, directors or the like who need to make the decision on killing a connection or keeping customers online. This is determined by weighing the costs of down time to lost revenues, clean-up time, customer trust, and business responsibility (as in SLAs). This step is extremely important and often forgotten, and if the response is improper it can have serious consequences. One example is an IT technician wiping a "routine virus" that has actually exfiltrated PII or PHI and not investigating further. This will most likely end up with lawsuits against the company for negligence or maintenance of improper security standards.

4. The next step is an attempt in containment. Once the proper parties, such as legal, business, and of course IT security have determined the scope and the nature of the breach, response may begin. Sometimes this occurs beforehand, usually by disconnecting the network cable or shutting down if data destruction is a risk, but such identification requires training. Containment's goal is not to remove the infection but to stop its spread, both from the outside and from internally. Often this is not done and lateral movement, the movement of traffic within the network from host to host as opposed to in and out of the network, overwhelms a team as the attack vector spreads.

5. Once containment is completed, the next objective is to determine indicators of compromise, data that was targeted, and potential motives and methods of the attack. This will help with classifying the attack and giving an appropriate response. Determining the motive can help understand what the goal was and give hints on how to find other areas of infection.

6. A preliminary response to this must be created and deployed. This involves the actual cleaning of the machines to a working order and removing the malware. It is to remove as much of the attack as possible before beginning the remediation phase and preventing further spread.

7. Bringing systems back up that were taken down requires careful planning. Any immediate security concerns should be addressed and remediated. These machines need to be cleaned and it must be ensured that they are ready for redeployment; otherwise, they may need to be scraped and made fresh again. While this is painful, it can help keep the environment secure and be a good excuse to move to more up-to-date systems.

Crisis communication becomes critical as soon as the company is aware of a data breach and activates the Immediate Response Team. The affected company needs to get out in front of the news and establish itself as the primary source of trustworthy information. A proactive crisis management perspective allows a company to control the messaging to the greatest extent possible. Of course a company cannot control how others may spin or spread the messaging, but the more it communicates clear, straightforward information of value, the better the chance of a positive outcome.

In the wake of a data breach, a company should focus on the following four strategies:

1. *Activate the crisis communications and management team*. Some believe that the crisis team should only be activated if it looks likely that a data breach will have a major impact on the company. This approach is not recommended. The crisis team should be activated whenever a critical event or a non-critical event that could potentially cascade into a full crisis is identified. As soon as an initial assessment determines the threat the breach poses, the team should be activated. All team members should have predetermined roles and responsibilities to enact per the crisis plan (see part one). To do their job properly, the team will need access to accurate, regularly updated information.

2. *Gather information*. Immediately after the alarm is raised about the data breach, the company should gather as much information as possible about what happened. This important process will impact how it manages the crisis, formulates messaging, and communicates to keep all parties updated and trusting in the business, its reputation, and its leadership.

As soon as the Immediate Response Team conducts a preliminary assessment of the data breach and its potential impact and damage (if possible), this initial evaluation must be sent to the crisis communications team so they can create the necessary messaging to proactively communicate with the company's stakeholders. Time is of the essence. In most circumstances all the facts will not be known at first. While this is normal and not a cause for alarm, lack of information must not be allowed to slow the communication process down. As new facts are gathered, they can be passed on to the crisis communications team for dissemination, provided the information is not sensitive and/or should not be divulged to the public as requested by law enforcement.

3. *Communicate honestly, openly and widely.* All parties, both internal and external, should receive the same messaging and information to ensure complete and absolute message uniformity.

Information used in the messaging must be based on what is known at the time. This is why it is so important to hold regular internal briefings among the IT team, crisis communication, and management team, executive management, and all external consultants and industry partners brought in to help address the unfolding crisis.

Messaging must include critical information that will answer media and stakeholder questions. In addition, the messaging should be completely open and honest and tell people what happened, how it was discovered, what was impacted, what the implications are for stakeholders, and what the company is doing to help those impacted. The company should communicate specific steps it will take to safeguard customers' interests, demonstrate that it understands the risks stakeholders face, and show that it has their best interests at heart.

While employees need to receive the information before it is disseminated to media and stakeholders, there should not be a significant lag time between internal and external communications. Companies must anticipate that their messaging will be leaked to external parties, which is why messaging uniformity is so crucial.

A core part of the communication process is to show that the company is open for communication by telling customers, stakeholders, the media, and individuals and companies directly and indirectly impacted by the crisis how to contact the company. People want to know that they can speak to someone for the duration of a crisis and thereafter. Giving parties a telephone number to call where they can speak to a real person can diffuse frustration and anger and minimize inclinations to rant and rave on social media or in the press. The company spokesperson should be available for media interviews at every possible opportunity.

Companies should leverage their social media assets with three objectives in mind: to proactively disseminate information, drive people to their website for more information, and monitor what is being said about the breach.

Regular updates are essential. Businesses need to frequently update their websites with new information, instructions, and news. Reliable updating helps prevent massive speculation and creates a sense of situational control. In certain cases, companies may need to adjust or curtail regular marketing activities to focus on the crisis.

4. *Monitor and respond*. Forward-thinking companies invest in reliable media and social media monitoring services or applications before a crisis hits. These tools measure social sentiment, provide critical intelligence, and allow companies to see what aspect of the data breach the media is covering and how various venues are portraying the company. Media monitoring applications provide companies the opportunity to respond to incorrect statements and rearticulate or change their messaging--all while remaining truthful and open--so that it better resonates with stakeholders.

In severe crises, the overwhelming volume of communication on social media platforms coupled with multiple stories in local, regional, and national media make effective technology-based monitoring and response solutions indispensable.

The way a company responds to a data breach, coupled with the messaging it transmits and the processes it puts in place to ensure that the crisis will never repeat itself, can determine its future viability and reputation value. Despite having the best plans available, a company can only walk away from a crisis with at least a portion of its reputation intact if it optimally handles the actual crisis management effectively.

In the next and final article, we will look at how companies can regain customer and stakeholder trust, and how they can best rebuild their business in the event they are hit by a data breach.

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

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