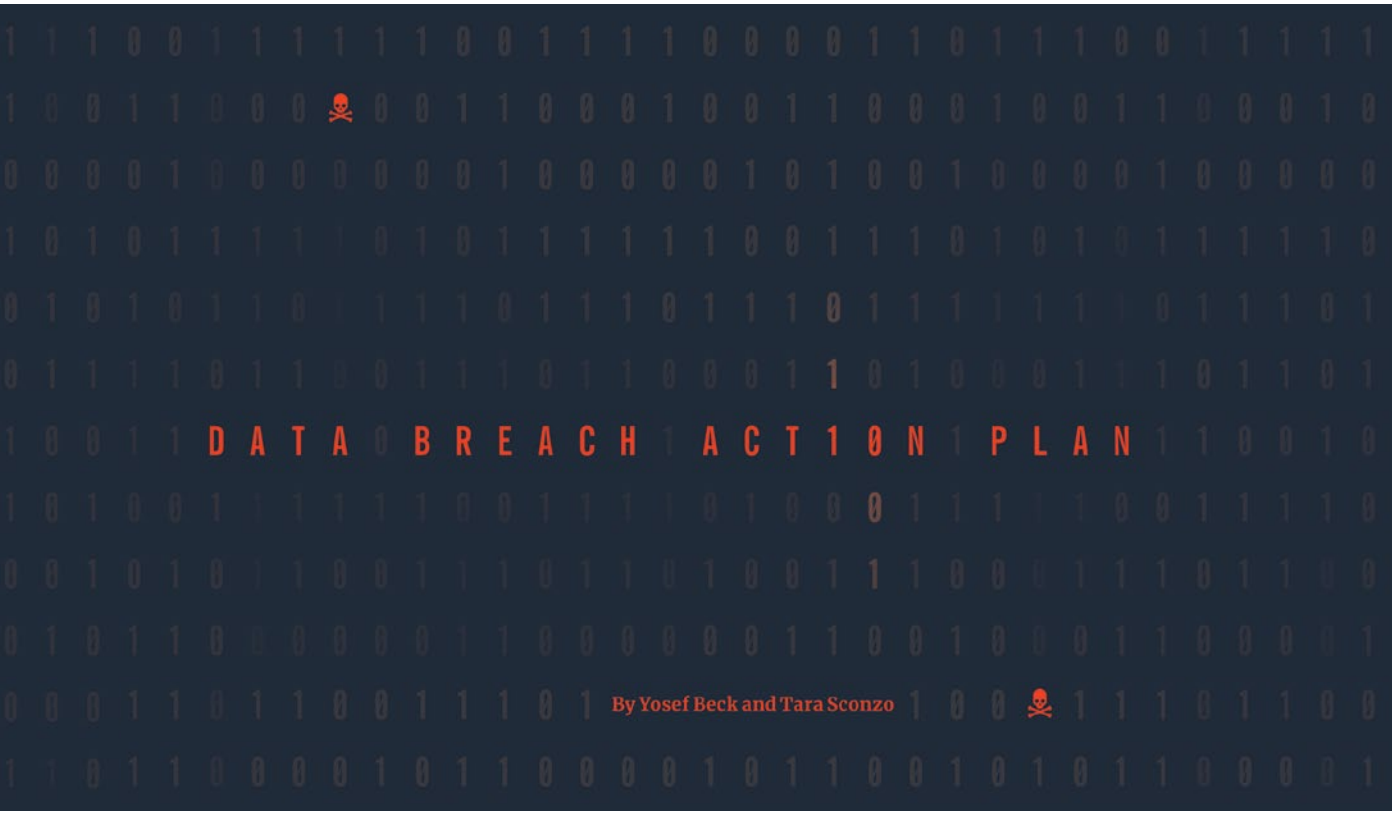


How your company responds to an incursion into your corporate or customer data can mean the difference between a disaster and a difficult PR problem.

2016 Average Incident Response Timeline

Source: BakerHostetler

69

DAYS FROM OCCURRENCE TO DISCOVERY

7

DAYS FROM DISCOVERY TO CONTAINMENT

Equifax, Yahoo, Arby's, Target, Home Depot, Deloitte, JPMorgan Chase, eBay, LinkedIn, Sony Pictures—it's a list of impressive companies that seems to grow by the day. What do they have in common? They all had to publicly announce data breaches that put customers and their personal information at risk.

At Jabian, we are helping CEOs, CIOs, and CISOs prepare and respond to data breaches around the globe. How a company responds can potentially make or break the company and its leadership (case in point: the near immediate resignation of Equifax's CEO).

A good response can increase brand prestige. It can delay or remove the risk of lawsuits. It can even lead to an increase in the company's stock price. These recommendations can help you right the ship if your company is the target of a data breach—and help you keep your job.

Make Sure You Are Covered

Data Breaches Can Happen to Anyone

In today's environment, it is almost a question of "when," not "if," a data breach will occur. Make sure you have a cybersecurity insurance policy—and understand it. To guard against insurance fraud, many policies will not allow a company to claim the time employees spend responding to an incident.

Ask your insurance provider if it has a reporting template or instructions for how to validate and provide proof of services rendered. Knowing this in advance and incorporating it into your action plan will help you and your vendors create the needed documentation throughout the process.

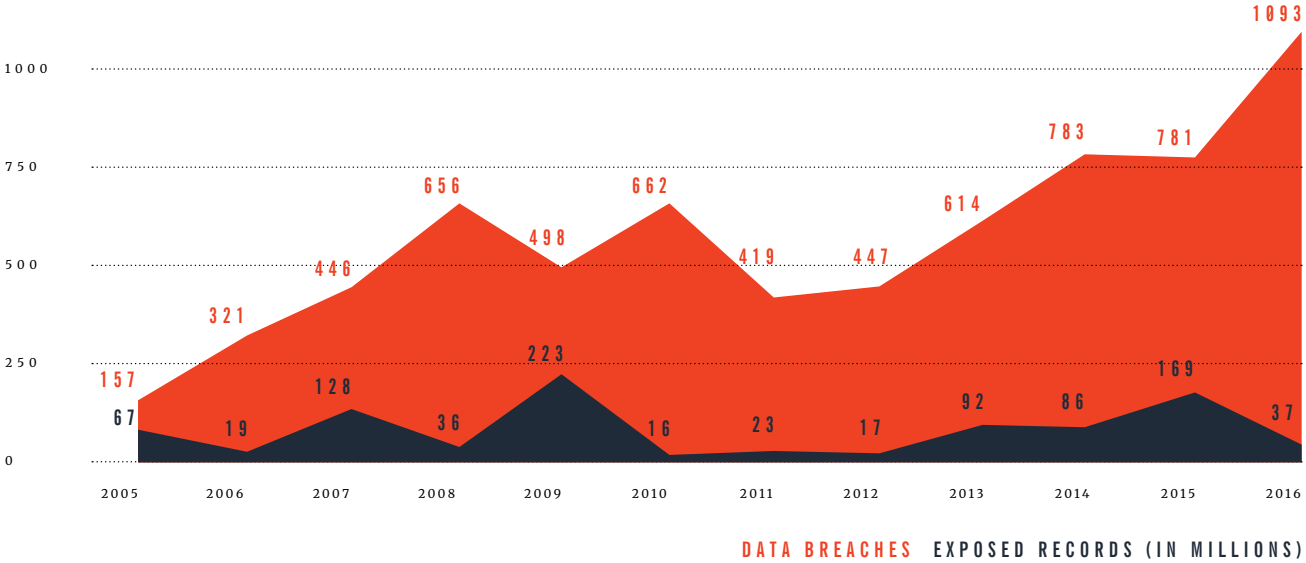
Having master service agreements in place with third-party responders before or immediately after an incident occurs can ensure you have the right people—with the necessary skills—available when you need them. Your insurance may even cover their help.

Be aware that insurance typically covers only the investigation, emergency containment activities, and notification of affected parties. Recovery is not typically included. It's assumed that doing those activities in the first place would have prevented the incident from occurring.

Don't forget about hard-copy records. As reported in BakerHostetler's Data Security Incident Response Report (BakerHostetler,

Number of Data Breaches and Exposed Records (in millions) in the United States

Sources: Identity Theft Resource Center; CyberScout



2016), incidents involving paper records accounted for 13 percent of all incidents in 2015. More common among health care incidents because of HIPAA requirements, BakerHostetler recommends that you ensure paper records, in addition to electronic records, are included in your information governance and incident response preparation.

Create a Plan

Preparation Is the Key to Managing Data Breaches

Once you become aware of a data breach, you have limited time and resources to react. Jabian's Data Breach Framework breaks down the pieces to include in your response strategy. The framework provides the flexibility to develop the plans you need in hand on Day 1 to address different data breach scenarios. You don't want to create your incident response plan while you are responding to the incident.

PRØJECT MANAGEMENT

A data breach requires many teams to come together swiftly and harmoniously. Having a project management office to orchestrate coordination is vital to surviving the data breach. In addition to the company's key executives, the response teams will typically include incident response, legal, external legal counsel, IT operations, third-party forensic investigators and responders, corporate communications, and the data/business intelligence team. Human resources may also be involved if employees are at fault or are the victims.

C0MMUN1CAT10NS MANAGEMENT

Having a dedicated resource focused on ensuring communications are sent to the press, internal teams, and externally affected parties is necessary. Unless you have drafted templates that are preapproved with legal (internal and external), you will need someone working full time in concert with legal to draft and wordsmith your communications to ensure the optimal message is delivered at the right time.

Your communications strategy should include internal and external stakeholders. There are many questions you need to think through, addressing: What will you communicate? To whom will you communicate? How much should you communicate? And who within your company is responsible for communicating? Are there any legal requirements for when you must communicate? If you are a public company, how could communications and timing affect your public filings or your reports to analysts and investors?

Informing your employees may sound like a good idea. A large percentage of data breaches, however, are caused by employees. If the data breach is malicious, you don't want to tip off the "bad guys" until you have time to gather evidence. Once you've collected your evidence, communicate a comprehensive response to employees about what happened and, more important, how the company will prevent this from happening again.

Like all the steps in a data breach response, ensure you're tracking internal communications—who receives them, when, and what is communicated—to ensure complete coverage.

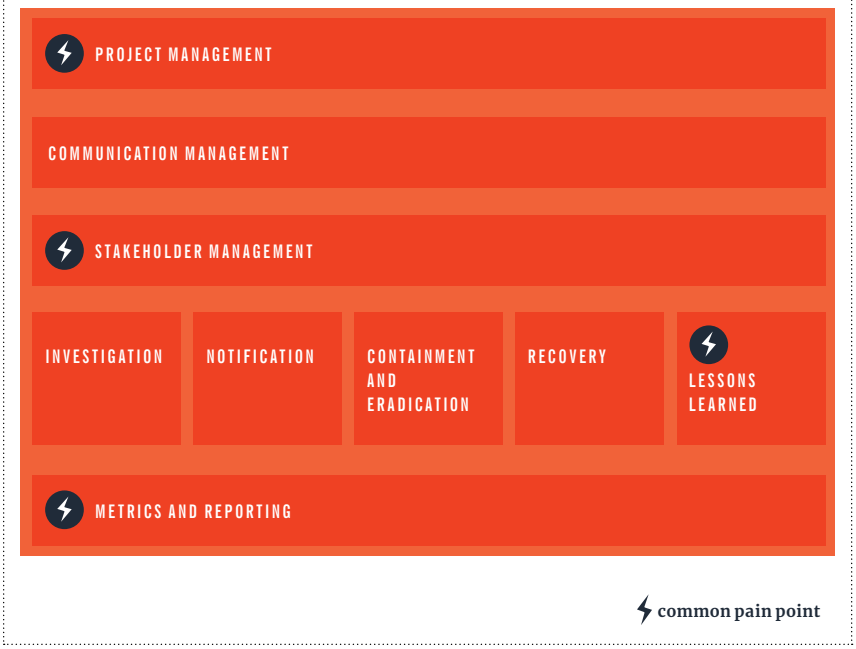
STAKEHØLDER MANAGEMENT

With regard to project and communications management, you must ensure that your critical stakeholders

are on the same page throughout the investigation, notification, containment, and recovery phases of a data breach. Have someone on point to ensure communications flow from the project management office and incident response teams to the appropriate stakeholders—internal and external.

You will more than likely have several vendors and internal groups working together across various work streams. They will need executive approval, as well as coordination with the correct internal counterparts (IT, legal, communications, etc.) to assist throughout the process. Coordinating with these stakeholders and groups can be time-consuming. It requires management, as speed of alignment, approvals, and delivery are important for the team to be effective.

Data Breach Strategy



1NVESTIGAT10N

The technical nature of the investigation will vary depending on the systems, networks, and data types involved. From a general process perspective, however, you must determine which systems are in or out of scope for the investigation; track what you have investigated and what is still in process; and understand when the investigation is complete. If you don't have the skills in-house, engage a private forensic investigation firm to investigate on your behalf.

If the credit card networks identified your company or some of your locations as being common points of purchase for credit cards linked to fraud, they may require you to use a forensic investigator certified by the credit card industry. The card networks will want to ensure it truly was a malicious outside attack, rather than an inside job, which could put your company on the hook for reparations.

Another difficulty may involve decentralized systems or systems that cross corporate boundaries (e.g., subsidiaries or franchises), which are not managed by a single corporate or IT unit. This fragmentation can lead to additional complications, as individual users and managers will have varying systems, programs, protection, and potential malware. Depending on your intercompany agreements, you may need to get permission from the subsidiary or franchisee before conducting your investigation. Ensuring up front that you have a well-thought-out cybersecurity clause in your intercompany agreements can provide a uniform and more timely investigation.

Keep in mind that individual system owners with proprietary knowledge and management of their computers, such as subsidiaries or franchisees, may be protective of their devices and be hesitant to engage outside help to investigate. They will be looking after themselves before the overall company, so you may have to offer incentives to get them to opt in to the investigation.

Incentives might include paying for the cost of the investigation or the cost of mailing notifications to customers. From the company's perspective, communicating all the information to the public in a single notification, which can quickly fade from the public eye, is a huge win. The alternative may be fragmented investigations (managed by individual parties) and multiple notifications that can drag on for months, if not years. Equally important is being able to centrally craft and manage the messages to customers and the public, ensuring they meet legal requirements and protect the company's brand as much as possible.

C0NTA1NMENT

As you identify issues throughout the investigation, you should work to immediately contain them without disrupting the investigation or damaging any evidence. The goal of containment is to stop the incident or the malware from spreading. At this step, the goal is not to remove or eradicate it.

Depending on the type of issue you identify, it may be possible to lock down your network or use an intrusion-prevention system to block the specific malware from phoning

ALL TEAM MEMBERS,0101
ESPEC1ALLY LEADERS,110
MUST BE C0MF0RTABLE01
TALK1NG AB0UT ERR0RS1
THEY MAY HAVE MADE0101

home even before you begin removing the issue. Or, you may be able to do a rolling remediation: As soon as the investigation of one system or location is complete, you remediate it before moving on to the next. Regardless of the timing, tracking is very important to ensure everyone knows the status of each system and location.

N0T1F1CAT10N

When you're sure you fully understand and have contained the problem, you can begin to identify and notify affected parties. As previously stated, you ideally want to send one notification to all affected parties to have the breach drop from the public eye as quickly as possible.

Legal review and approval of the notification is critical, as there are unique requirements for states and countries, which may also depend on the point of purchase. In addition, consult key stakeholders to determine how to craft the message to best represent your brand, addressing questions such as: Should you use company letterhead? Who should sign the message? How should you address the customer?

ERAD1CAT10N

Once you've completed the containment phase, begin to eradicate the issue. The goal is to fully reverse the damage or remove the malware from the affected systems; it is not to fully recover those systems back into production. This step should follow your standard IT change management process to eradicate the issues from the affected systems (e.g., upgrade and patch software, reinstall base operating system, set up and migrate to new hardware, etc.) as well as minimize any identified vulnerabilities or risks and harden the affected systems.

REC0VERY

Once the damage is eradicated, you can restore lost functionality and data and remove the temporary containment measures you may have left in place. Steps include testing the restored and hardened systems, deploying them into production, monitoring systems for signs of incident reoccurrence, validating that the systems are fully recovered, and removing any unneeded containment measures.

LESS0NS LEARNED

Don't leave out this last step! Take this opportunity to learn from your experience by improving and standardizing your data breach response process to be better prepared in the future. Hold a "lessons learned" meeting within one week of the close of the incident to ensure everyone's activities and thoughts are fresh in their minds.

Make sure everyone checks their feelings at the door. All team members, especially leaders, must be comfortable talking about errors they may have made. The focus of the meeting should be on team performance. Be open with congratulations and constructive with criticism while examining every phase of the operation. The result of your meeting should be a list of identified probable causes of any identifiable errors, so you know what could be done differently to improve the result next time.

METR1CS AND REP0RT1NG

As you may now realize, the response to a data breach includes a lot of moving parts. Having standard templates that allow quick and clear summation and communication, especially during the hectic first days of the response, can be critical. Having a team of reporting specialists who are familiar with those templates, and who quickly grasp what is important to track and what noise to filter out, is equally imperative to enable executives to make the requisite decisions.

A final thought to incorporate into your response plan: As data and reports are passed around among different teams, ensure that you're sending documentation securely. It would not look good if your data breach response team caused a second breach!

Yosef Beck
yosef.beck@jabian.com

Tara Sconzo
tara.sconzo@jabian.com

Works Cited: *BakerHostetler. (2016). Data Security Incident Response Report. BakerHostetler. Retrieved from https://bakerlaw.com/files/uploads/Documents/Privacy/2016-Data-Security-Incident-Response-Report.pdf*