SECDO

BE SECURITY BREACH-READY

—

CREATING AN EFFECTIVE RESPONSE PROGRAM FOR INEVITABLE SECURITY BREACHES

CONTENTS

EXECUTIVE SUMMARY

HOW READY IS YOUR COMPANY FOR THE INEVITABLE BREACH? ARE YOU ABLE TO RESPOND EFFECTIVELY? WILL YOU BE ABLE TO COMPLY WITH REGULATORY REQUIREMENTS?

Headlines are full of alarming news about security breaches and the mayhem they cause to victimized companies and their customers. Yahoo, Target, EBay and Sony are names that are bandied about in discussions about the scourge. Patient data, financial information and industrial secrets are held for ransom or posted publicly. The public cries out for help.

Governments and their behemoth body of regulators jump into the fray and create tomes of laws and regulations to which entire industries are subject. HIPAA, PCI DSS, SOX, FISMA, GDPR and a host of other initials and acronyms now fill the data-security landscape, sending companies reeling to comply.

Due to recent horrific security breaches and theft of data, regulations are getting significantly tighter. Companies are now required to hire senior data-security officers with staffs to set up and monitor far-reaching data-security programs that must undergo regulatory approval. The latest regulations hold companies responsible for full disclosure within 24 or 48 hours of a breach. Lack of compliance can mean severe fines and penalties.

This paper is brimming with good advice to help you make your company security breach-ready.

STATE OF READINESS

Ill-prepared companies unwittingly step into the quagmire of a breach, sinking ever deeper as they labor in vain to extricate themselves. Sadly, this seems to be the most apt description of the state of security-breach readiness.

When the inevitable occurs, companies are caught unawares and discover—too late—that their response is inadequate. Disaster looms ahead in the forms of customer loss, class-action lawsuits, and irate regulators showing up at headquarters.

DREAD

THE OMINOUS BREACH APPARITION CAN APPEAR IN VARIOUS MANIFESTATIONS. THE MOST BENIGN VERSION IS WHEN ONE OF THE COMPANY'S OWN MONITORING SYSTEMS DETECTS SYMPTOMS OF A BREACH AND THE SECURITY TEAM CAN ADDRESS IT IN FULL BEFORE NEWS TRICKLES OUT.

The dreaded manifestation is notification from an external agency, typically law enforcement, informing you that data is leaking. (We're being kind here. The tone is usually accusatory, full of regulations that are being transgressed and accompanied by the dire consequences that are crouching at the door.)

Alas, despite considerable efforts, time and expense – expert advisors, staffing, training, processes, technology – sensitive data has escaped and you didn't even know about it. The myriad controls that you put into place may have been highly successful until now, detecting and preventing hundreds of potential breaches, but never mind that. While attackers are allowed to fail 99.9999% of the time, you need to fail but once to be on tomorrow's front page.

Upon discovery of the breach, the security team must quickly brief management who has precious little time to format a report to the riled regulator. There are many questions your CEO, the regulator and the public want answered:

IS THE BREACH STILL HAPPENING?

WHEN DID THE BREACH START?

WHO IS INVOLVED?

HOW DID DATA LEAVE THE COMPANY?

WHICH RECORDS WERE EXFILTRATED?

WHAT IS THE ORIGIN OF THOSE RECORDS?

WHERE DID THE DATA GO?

The mere creation of the initial report sends the security team and, in some cases, the entire company, into complete chaos. Red alert! We have an emergency! And it's all hands on deck when panic takes over.

SCOPING AND CONTAINING THE BREACH

HOW AWESOME WOULD IT BE TO JUST CLICK A BUTTON AND MAKE THE EXFILTRATION STOP? TO CLOSE ALL OUTBOUND CHANNELS AND KNOW FOR SURE THAT THE LEAKS HAVE BEEN PLUGGED?

Assuming that the leaked data is digital (as opposed to hard copy or people), you could simply kill the power supply to the entire company, shut down the network, and halt all access. That ought to work. But since that's not realistic, the first item on your list must be the quick collection of preliminary information that helps you understand the basics: what happened, is it still happening, where. You must scope the incident correctly to contain it.

Are you sure that data leaked? What data exactly? Which endpoints and servers are affected? What evidence must you collect to conduct an effective investigation? How do you go about collecting it?

Getting the scope right at the outset can make the crucial difference between successful containment and unmitigated disaster. Miss important evidence and the entire battle could be lost before you even get a chance to fight back.

In so many cases, inadequate scoping is the major failure that destroys any chance of success. Security teams are so eager to prove that they are up to the task that they tend to respond prematurely before fully understanding what they are responding to. Scoping requires time and effort. Doing it right can lead to a successful outcome.

After scoping the breach, you must try to contain it by blocking communication channels, taking machines off the network, disabling users and the like – all in the interest of protecting the company, reducing panic levels, and showing that you are on top of the situation.

GATHERING EVIDENCE

ASSUMING YOU MADE IT THIS FAR, YOU MUST NOW LOOK FOR EVIDENCE.

Terms like logs, packet captures, bit-by-bit duplication of hard drives, memory dumps and forensic analysis are high on the list of commonly used words that you will hear at this juncture.

Time is of the essence. Digital evidence is volatile. The more time has passed, the less likely you are to collect the data you need. But management and the regulator want a reply ASAP. How likely are you to provide answers in a timely manner?

Here are the appropriate questions: Is all the evidence even still available? If so, can you acquire it? Will it help you once you have it?

While many companies collect logs in a log management system or SIEM, and some even record raw packet data, often, some critical evidence is missing: logs or packets are no longer in retention or are simply unavailable.

Memory or disk forensics can be helpful, but these types of evidence tend to be highly volatile, disappearing in a flash. They are elusive and a lot harder than logs to understand and analyze.

So, despite the best efforts of your talented security staff, complete answers are rarely available in the allotted regulatory or damage-control time frame.

ANALYSIS

YOU ARE NOW FACED WITH THE DAUNTING ANALYSIS. DO YOUR PEOPLE HAVE THE EXPERTISE TO SWIM THROUGH DEEP DATA POOLS TO NET CRITICAL CLUES?

READING LOGS IS ONE THING, BUT UNDERSTANDING THE STATIC ANALYSIS OF CODE IS A WHOLE DIFFERENT GAME.

Context matters. Gathering evidence was hard enough, but putting it into proper context for effective analysis can cripple the entire effort and leave you bereft of answers.

True and complete analysis performed properly can take days or even weeks, depending on numerous factors like the nature and volume of the evidence, the tools available and verification of the results. Under pressure, the good-willed analyst might bull his way through the data too quickly, missing the smoking gun hiding in plain sight. None of this bodes well for compliance with short regulatory time constraints and shorter tempers. In the attempt to speed things up, security teams may damage the very evidence they will need later, violating an axiom of forensic investigation: Maintain the integrity of the evidence!

"Not invisible but unnoticed, Watson. You did not know where to look so you missed all that was important."

Sherlock Holmes

Hard-pressed to deliver quick answers, analysts can provide only a fraction of the story, so they simply fill in holes with guestimations. You are left with three major problems:

- Answers provided are simply incorrect; you might be feeding the regulator false information.
- Without understanding fully what took place, you will never be able to completely fix the breach and prevent it from reoccurring. It WILL happen again.
- The evidence that you may need later for deeper analysis is damaged in the collection process and rendered worthless for future use.

Faulty analysis might be worse than no analysis at all.

ENTER THE EXPERTS

SOME COMPANIES UNDERSTAND THAT THEY ARE NOT EQUIPPED TO HANDLE BREACHES OF EVERY LEVEL, SO WHEN THEY ENCOUNTER A PARTICULARLY PERPLEXING AND DAMAGING ONE, THEY BRING IN THE BIGSHOTS, THE GUNSLINGERS OF CYBERSECURITY – EXTERNAL CERT/CIRT TEAMS.

These expensive black-belt, master-ninjas can do it all – assuming that they arrive quickly enough and can get access to the data they need.

The worst thing you can do is to call them in AFTER your team has conducted its own analysis and damaged precious evidence, producing scowls and accusations from the ninjas: "Why did you touch that?" and "How do you expect me to figure this out when you wiped the evidence?"

If you need the experts, get them into the fray ASAP. It's a good idea to get to know a few personally (and even have SLAs in place) before your breach. If you arouse them in the middle of the night with your fresh disaster, they might not respond quickly enough and are certainly likely to charge you an arm and a leg. They can smell fear. Under duress is not your best moment to cut deals with strangers who are the only game in town.

External CERTS are not the be-all, end-all. You still run the show. You will need to coordinate the entire operation and provide them with whatever they need (pizza, stuffed animals, access to the company's secrets). They need direction.

POST-BATTLE REPERCUSSIONS

THE SMELL OF BATTLE PERMEATES THE AIR. A GLANCE BEHIND REVEALS ACRES OF SCORCHED EARTH. BUT YOUR WEARY SOLDIERS HAVE TRIUMPHED. YOU HAVE CONFRONTED YOUR DEMON AND SURVIVED.

But you aren't done yet.

There are lots of important people to update: company management, regulators, customers, partners, suppliers, investors, shareholders, the media, and more.

What about the company's reputation?

While you may be able to calculate how much each piece of lost data cost and how much was paid out to the ninjas, the damage from a bad reputation can be incalculable. Only time will tell. Target and Yahoo are still reeling from breaches that occurred years ago.

If you're lucky, you may not suffer any such drastic damage, but that's not typically the case. Today, everybody is becoming aware of data-privacy issues. People care where their information is, who is using it and how. Losing data that they trusted you with may lose their trust in you!

RETURNING TO NORMAL

AFTER THE WAR, SOLDIERS HAVE TO GO HOME. YOU'LL HAVE TO RETURN TO YOUR AND YOUR COMPANY'S DAILY ROUTINE. CAN YOU DO THAT AFTER A SERIOUS BREACH? CAN YOU RESTORE FAITH?

Your company can never be the same.

Breaches, and dealing with them, reveal flaws in the way a company goes about its business. Shortcomings can be found in business-related systems, how they are implemented, tested and maintained. There are myriad other reasons to consider such as missing or unfollowed policies, faulty decision making and improper prioritization.

You will have to make sure that the business units are able to work safely and that the gaps in the security layers of the company are properly attended and fixed. This, of course, will require more technologies, processes and people. (Maybe this time, when you ask for more budget, the boss will be more understanding.)

LEARNING FROM EXPERIENCE AND THINKING AHEAD

You are not alone. Target, Sony, Home Depot, RSA, Lockheed Martin, EBay, Yahoo and numerous others have all been there. Did they not spend millions on security? Weren't they breached anyway?

The lesson is: it WILL happen again.

With this lesson clearly in mind, you will understand that the question has shifted from "how to prevent" to "how to respond effectively".

Move your focus to response.

Merely defining "effective response" is, in itself, challenging. It necessitates being efficient, thorough, and timely. To become a nimble and effective responder to inevitable incidents, here is what you should do:

01 PLAN AHEAD

In grade school, children learn what to do in case of an earthquake. No one can control the tectonic plates under the Earth's crust. We struggle with predicting the magnitude or exact location or time, but no one doubts the fact that the Earth will shake from time to time.

The same idea applies here. By all means, spend money making your company more secure. But understand that nobody can control hackers and your network will be breached. So, plan to make your company breach-ready.

The plan must be corporate-wide, not just for the security team. It should emphasize people and processes with only minor focus on technology at this point.

Create and implement a **Breach Management Plan** and get it authorized by senior management. Security breaches tend to have corporate-wide implications so relevant departments and people should all be involved in the plan. They may include spokespersons, HR, Legal, Physical Security, IT, Audit, and more. Your job is to make sure that everyone who is involved knows his part and can act according to his role, responsibilities and SLAs.

02 DEFINE WHEN AN INCIDENT BECOMES A BREACH

Security events, alerts and even serious incidents are handled by security teams every day. Outside of routine, high-level reports, management knows very little of the ongoing security operation and expects the security team to function properly, handling the security matters that come before it. This is why you're here.

Breaches are different. They scare your customers. They chase away your suppliers. They can affect the business and reputation of the company. When a breach is detected, you need to notify senior management. That's exactly why you must define what a breach is.

The definition of a breach will differ depending on country, industry, regulatory requirements, company size, and other factors.

Typically, a breach relates to personally identifiable information, data mentioned in regulations or anything that was determined to be critical during a Business Impact Analysis. The very people you will be working with on the creation of your Breach Management Plan will help you define a breach.

03 ENGAGE EXTERNAL TEAMS

While building the plan, you may realize that there are areas you are not able to address. They may include high-level security experts, and, in some cases, may require an external PR consultant or additional legal assistance. Identifying skill gaps will allow you to address them correctly and incorporate solutions in the plan itself. You will define exactly when you need to call for outside help, who it will be and what services you expect.

Select good, long-term service providers and enter into agreements that clarify the services, prices and the SLAs you expect. It is highly recommended that you choose more than one provider for each area of expertise or service that you will need. You might need choices. When the breach happens, you can't wait for somebody to return from vacation.

04 PRACTICE MAKES PERFECT

As every athlete knows, in order to be at the top of his game, he must practice, practice, practice. No shortcuts.

Breach management is no different; it must be practiced several times before you can be sure if is good enough for the big leagues. Then, it must be reviewed and re-practiced periodically to keep it sharp. When a real breach happens, all the time and effort spent on practice will prove itself as the breach will be properly managed end to end by people who now have experience.

Practicing the plan will reveal action items that might look good on paper, but work less efficiently in reality. If something doesn't work when you try it out, revise it and try it out again until it achieves the level of effectiveness that you need.

A good way to practice breach readiness is penetration testing. Penetration testers can challenge the resiliency of your security defenses and how well you handle breaches.

05 COORDINATE BREACH RESPONSE

Breach-readiness is a complicated process. Like a football team, you must sync all the players—departments, individuals, senior management, experts, consultants—making sure that everyone knows exactly what to do and when. Get to know the people you will need to call on in times of emergency and be ready send them into the fray.

You are the coach of the breach-response defense. Charged with repelling the offensive attack, you need to bring your A-game. You are rallying your team out of the trenches. You will have to coordinate the gathering, analysis and sharing of useful information effectively, efficiently, thoroughly and timely.

06 PREEMPTIVE BREACH RESPONSE

You must not rely on post-mortem collection of data/evidence in the wake of the breach. It's too late. You must collect it from all available sources all the time, and model it so that it will be easily accessible to you and your team when the breach occurs and you are under pressure.

This is the reason why companies collect log information in SIEM or Log Management systems. The idea is to have data available in one place for a long period of time, just in case you need it. But it's not enough. Logs are typically too lightweight to help you effectively in the aftermath of a breach. They usually contain information only about the symptoms – not the root cause – of a breach. They do not contain enough data to do complete damage assessment – one of the major elements that the regulator wants to see.

Whenever there is a breach, or even a minor incident, security teams go to company endpoints and servers for answers. Gathering evidence from endpoints and servers enables incident-response team to piece together the steps of the breach. In many cases, by the time analysts get to the endpoints and servers, the evidence is gone due to the nature of volatile memory.

Therefore, you must collect forensic information from all endpoints and servers 24/7/365 and store it centrally for a long time. Since endpoints and servers are where everything happens, they hold the keys to determining root cause of the breach and precise damage assessment. This forensic information must be available immediately upon discovery of a breach.

Preemptive data collection readies the evidence necessary for the breach-response process. Done right, this concept can turn weeks of painstaking work into 10 minutes of pivoting data around a screen. Using this information that you have already collected and have at hand, you are able to properly scope the breach and perform complete damage assessment. You can contain and remediate accurately. These actions are expected to be technical and may require the joint efforts of several teams working together to make sure the breach is completely defeated and that there are no vestiges that could damage the company yet again.

Preemptive Breach Response is all about saving time when you need it most, providing the effectiveness, efficiency, and thoroughness you need for breach management. This methodology is the key for complying with regulations concerning timely auditing and reporting.

---

07 REPORTING

Prompt sharing of accurate information with the right people expedites breach response and post-breach learning and improvement. Participants in the process depend on the security team's findings to know how they succeeded or failed, contributed or got in the way.

However, it is important not to over-share information about the breach as this can do greater damage than the breach itself. Why do customers need to know about a breach if you caught it in time and their personal identifying information never leaked?

With Preventive Breach Response, since you are able to handle the breach quickly and completely, you can report back only to the relevant stakeholders without over-exposing the company or creating unnecessary distrust.

Your report should include:

- What exactly happened from start to finish?
- How did the breach start?
- What was damaged or stolen?
- How did data leave the company?
- Where did the data go?
- How did your team handle the incident?
- What do you plan to do to make sure it doesn't happen again?

CONCLUSION

WE NOW LIVE IN A WORLD WHERE CYBER BREACHES ARE A FACT OF LIFE. WHILE WE NEED TO SPEND TIME, EFFORT AND MONEY ON PREVENTION, DETECTION AND OTHER PROTECTION SYSTEMS, BREACHES WILL CONTINUE TO PLAGUE US. SOMETIMES, THESE BREACHES CAN BE CATASTROPHIC.

When a breach inevitably occurs, we must race into action. We must minimize damage and then quickly restore our environment to its pre-breach working state. The process of responding to breaches must comply with strict regulatory requirements.

For these reasons, it is vital to create a company-wide Breach Management Plan that includes all the processes and procedures necessary to react efficiently to any incident and to comply with regulations. The plan must be practiced in order to maintain its effectiveness and currency.

The company must be on a 24/7/365 breach-readiness footing, prepared ahead of time for the inevitable. It must collect endpoint and server data continuously and put it into context so that it will be available for analysis, enabling you to respond rapidly and correctly to any breach that happens.

Follow the advice in this paper and be security breach-ready.

SECDO

PREEMPTIVE INCIDENT RESPONSE DONE RIGHT

SECDO's Preemptive Incident Response solution slashes incident response time to minutes. Gain unmatched historical thread-level endpoint visibility, automatically investigate any alert and visualize the forensic timeline and attack chain back to the root cause. Then, remotely and surgically respond and remediate on any endpoint or server without impacting business productivity.

HIGHLIGHTS

- End-to-end Incident Response time is drastically reduced
- Security teams handle far more alerts in far less time
- Alert fatigue is shredded
- Investigations are lightning-fast, intuitive and accurate
- Remediation is rapid and precise
- Defenses are improved and future attacks are thwarted

REQUEST A DEMO