5 STEPS TO WEATHER THE “ZERO HOUR”

SUMMARIZED FROM “THE ZERO HOUR PHONE CALL: EXPEDITE YOUR DATA BREACH RESPONSE TO MINIMIZE RISK”

BY SHERYL FALK, PARTNER AT WINSTON & STRAWN
Perhaps your InfoSec team found a malicious code wreaking mischief upon your network. Or maybe the FBI called to report that your organization’s data has been hacked. Either way, you have entered the “Zero Hour.” There is a security breach of your network and you must respond—now—because sensitive data is at risk.

If the Zero Hour strikes your organization, here are five steps to help you make faster decisions and return your endpoints back to a trusted state:

1. **Understand Your Data**
   - It is critical to have a firm grasp on your data—especially your most sensitive information—and where it’s stored. This basic precaution will be invaluable in the event of a breach. Remember, not all of your data needs to be shared outside of your environment. Some organizations have their own internal networks, and do not rely on data connected to the Internet. This greatly reduces the risk of compromised information.
   - If some data has more value to you, consider caching it in a highly secure, less accessible place. Here are a few guidelines to keep in mind:
     - Understand where your data is and how it is protected
     - Depending on the location, different laws may apply
     - Classify your sensitive/proprietary data
     - Use a data map to track the whereabouts of your most valuable information

2. **Evaluate and Update Your Data Security Policies**
   - You may already have data security policies, but is it time for an update? Policies need to change and evolve over time to maintain industry standards. And merely having guidelines isn’t enough. You need to educate stakeholders about the protocols, as well as monitor and enforce them.
   - Here are a few policies that should be at the top of your company’s security list:
     - Vendor access and storage policy
     - Remote access policy
     - Internet and electronic communications policy
     - Social media policy
     - Password policy
     - Mobile device policy
     - Guest access policy
     - Network device attachment policy

3. **Plan Your Data Breach Response**
   - Fully plan your counterattack to a data breach, beginning with identifying your internal response team and external response partners. The latter is especially important: The middle of a breach is not the time to argue over indemnification clauses. The key stakeholders should know and be ready to execute the plan. It’s a good idea to practice your plan in a tabletop exercise to judge the response and effectiveness.
   - When you’ve identified your security and forensic experts, you can respond quickly when the Zero Hour strikes. You should be able to open your plan, see who you need to call, and know who has already signed a Terms of Agreement so that everyone can proceed immediately.
   - We suggest these experts be available for emergency access:
     - Key IT administrators
     - Law enforcement contacts
     - Security experts
     - Forensic experts
     - External privacy counsel
     - Communications/public relations/notification support
Do you have cyber liability insurance coverage? The SEC not only requires that you disclose a material breach, but that a breached company discloses any relevant insurance. Find out specifically what your general business liability plan covers. Some case law states that cyber liability exclusions prohibit insurance under a business liability policy. There are some courts, however, that recognize a server as tangible, and subject to coverage under such policies. In these cases, compromise of a server might be covered. It is imperative that you understand what your policy says with respect to cyber liability.

Likewise, if you have a separate cyber liability policy, you also need to understand what it covers. There are many expenses that could be incurred such as cost of lost business, investigation, forensic and legal investigation expenses, credit monitoring, legal defense of lawsuits, civil fines, and class action lawsuits. Your policy may require you to work with certain security vendors or forensic vendors, and to adhere to particular standards to have the insurance in check.

Understand what you are telling external stakeholders regarding how you will take care of their data, and make sure your representations are up to date and accurate. Here is what one well-known company proclaims:

“We aim to provide you with the world’s strongest security and privacy tools. Security and privacy matter to us, we know how important they are to you and we work hard to get them right.”

The statement aims very high. The well-meaning company is promising to care for its data with “the world’s strongest security and privacy tools.” If there is a material breach with litigation, the prosecutor is going to key on this statement, portray it as misrepresentation, and use it in a damaging fashion against the company.

Such assurances could be considered overpromising the level of data protection your clients have from your organization and could do more damage than good in the long run. As security challenges evolve, how you respond must evolve as well. Check your representations so they are up to date and accurate.

CONCLUSION

A Japanese proverb states, “The reputation of a thousand years may be determined by the conduct of one hour.” Don’t let the Zero Hour ruin your hard-earned reputation! You probably already know that it’s not a matter of if you’ll be hit with a data breach, but when your Zero Hour phone call will ring.

Remember, there’s power in planning. In addition to these five steps, reliable incident response tools are needed for when the Zero Hour phone call happens. Guidance Software is the maker of EnCase, a proven endpoint detection and response tool relied upon by organizations and agencies throughout the world. With EnCase Endpoint Security, you can quickly validate and triage incoming alerts, have complete 360° visibility across the enterprise, and surgically remediate all instances of a threat. The result: complete confidence in the event of a breach.

Learn more at guidancesoftware.com

For the full paper “The Zero Hour Phone Call: Expedite Your Data Breach Response to Minimize Your Risk” by Sheryl Falk, Partner at Winston & Strawn download here.
Five Steps to Weather the “Zero Hour”

ABOUT GUIDANCE
Guidance exists to turn chaos and the unknown into order and the known—so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.

Guidance Software®, EnCase®, EnForce™ and Tableau™ are trademarks owned by Guidance Software and may not be used without prior written permission. All other trademarks and copyrights are the property of their respective owners.