Six Steps to Protect Evidence and Address Issues After a Cybersecurity Breach

Let's face it—cybersecurity problems can affect businesses of all sizes in all industries. In fact, Verizon's 2018 Data Breach Investigations Report made this especially clear when it revealed that more than 53,000 incidents and 2,216 confirmed data breaches impacted organizations worldwide last year alone. While breaches can be devastating for your business, they can be equally lethal from a litigation perspective. Messages, attachments, and other data pertinent to ongoing or pending litigation could be considered inadmissible if these forms of evidence are deemed corrupted. Your business can even face sanctions. Especially if the data breach event was perpetrated by an insider, ex-employee, or was expedited by your organization's internal document management practices.

Taking Action to Protect Evidence

So, what should your business do in the event you're forced to confront a critical cybersecurity incident? Here are some immediate steps you and your in-house counsel can take to protect critical electronic evidence from ending up inadmissible.

1 Assemble Your Incident Response Team to Contain Breach Activity

If your business has just discovered cybercriminal activity on your servers, it's highly likely that it's been going on for some time. As a 2018 IBM/Ponemon Institute Study revealed, it usually takes companies 197 days on average to discover ongoing data breaches, and an additional 69 days to successfully contain them. Acting quickly to respond to breaches could end up saving millions. You should activate your incident response team as soon as possible.

Your team should ideally consist of IT staff members with open access privileges; outside forensic and cybersecurity consultants who act under the direction of your legal counsel; representatives from various internal corporate departments; dedicated in-house counsel contacts; and pertinent C-Suite executives such as your CISO, CIO, and CSO. In addition, your team should have dedicated communication channels in place that are monitored by your legal team, which allow your attorneys to provide real-time input on important breach response decisions.

Once your team has identified affected accounts and databases, consult with your forensic consultants and attorneys to determine next steps for retrieving pertinent data and isolating impacted servers.

2 Use eDiscovery Software and Other Tools to Better Understand What Information Could Be Affected

eDiscovery tools may have been designed for litigation, but they can often be just as useful for locating critical files and helping your team understand how those files are organized within your information governance (IG) infrastructure. Some programs allow you to use keyword-based, file-type-based, and structured data searches to see where data is being hosted within your company. These searches can help your team better prioritize not only which accounts and databases to investigate for suspicious activity, but also which specific emails, files, images, and other potential evidence need to be collected and preserved to avoid corruption. You can also generate permission reports to see which individuals had access to these files. This can help not only alert IT to potential vulnerabilities and backdoors within your user accounts, and help your in-house and outside counsel locate contacts to interview about the breach. To minimize your data loss risks if you decide to try accessing infiltrated servers, you should only do so with the help of experienced cybersecurity and forensic consultants. Especially if the breach is active and ongoing.

3 Confirm Whether Files Critical to Open Case Files Could Have Been Affected

If you already have active legal holds and cases in place, work with your IT department to determine whether any custodian accounts currently under investigation are at risk. If so, circle back with your IT staff to freeze routine data retention and deletion account settings and ask custodians whether copies of pertinent ESI evidence are being stored elsewhere. To fend off criminal insider activity, you should limit server access privileges to only authorized response team members, executives, employees, and law enforcement personnel.

4 Check for Changes to File Metadata and Chains of Custody

Even if the electronically-stored information (ESI) you've recovered appears to be fine, you'll still need to see whether files were altered or compromised on a deeper, more technical level. File metadata embedded within your ESI can reveal this, particularly since this metadata can shed light on file version histories and contributor information. Your business must also show that your ESI files were not mishandled or altered between the time they were created and the date of production. Documenting chain of custody and keeping them intact can help establish the integrity of retrieved ESI you later submit into evidence.

ENSURING AUTHENTICITY, COMPLETENESS, RELIABILITY, BELIEVABILITY, AND ADMISSIBILITY OF EVIDENCE

Scene of the events

what	when	where	who	how	why
Is the nature of the evidence? Is its source? Is the type of data? Is the amount of data?	Was the evidence created Was it collected Was it examined Was it transferred to other custodians or storage locations	Was the evidence collected Was it stored Was it examine	Created the evidence Found it Collected it Owns/Manages it Handled it Has access to it Accessed it Was involved throughout the process	Was the evidence found Was it collected Was it preserved Was it secured Was it examined Was its integrity maintained?	Was the evidence collected Was it examined

Courtroom

netgovern™

5 Document How Your Organization Responded to the Incident

While it may sound cliché, it really works to leave no stone unturned when documenting your breach response activities. Although breaches can happen to even to the best-prepared businesses, they can force courts to question the defensibility of your existing IG practices and data retention procedures. Particularly if your current practices facilitated the corruption or loss of important files. This will be especially true if the breach was intentionally committed by insiders, which could possibly leave your business susceptible to sanctions.

Be sure to preserve activity logs for your servers and programs and conduct interviews with executives and employees who helped investigate and contain the breach. Also make sure to compile lists of current and former personnel who may have had access to pertinent servers and databases. Your team should also document whether the breach led to any loss of ESI evidence or other server and hardware damage.

6 Notify Opposing Counsel About Developments Involving Evidence

While it's likely that you'll need to send data breach notices to your customers and relevant government agencies to satisfy your privacy law obligations, you may also need to advise opposing counsel about the availability or destruction of specific ESI. Work with your in-house and outside counsel to determine whether you can provide lost ESI files in other accessible formats, as well as how to best respond to subsequent requests for production, admission, or depositions. Depending on your situation, you may also need to formulate strategies for fending off requested sanctions for intentional or bad-faith activities involving irretrievable ESI.

Forewarned is Forearmed

Waiting until you've had a major security breach to put a cybersecurity breach response protocol in place is a lot like locking the door after the horse has bolted - suboptimal. Long before you identify a breach you need to assemble a team, put procedures in place and make sure you have the right software to help you respond. Being ready ahead of a crisis could save you millions.

See how NetGovern can help you stay one step ahead when it comes to protecting critical ESI evidence.

netgovern™

Talk to one of our experts about Data Protection and Information Governance: netgovern.com