Supplement to the Los Angeles and San Francisco
Daily Journal
JANUARY 24, 2018

TOP CYBER/ARTIFICIAL INTELLIGENCE

Hacked? Don’t waste time pointing fingers

By Daniel Garrie and Michael Mann

Cybersecurity attacks, data breaches and hackings can be devastating and demoralizing to a company, leaving it with a difficult question: What now? Too often, companies focus on the whodunit of a cyberattack. They want to attribute the data breach or cybersecurity incident to a specific actor, a villain. Yet focusing an internal investigation on identifying the source of a data breach or cybersecurity attack is often an inefficient use of the company’s time and resources.

Consider the following scenario. You are coming home from a vacation with your family. When you reach the front door, you notice that the door is unlocked and the door jamb is completely busted. You push open the door further, only to find the house in complete disarray. You quickly put the pieces together and determine that while your family was enjoying vacation, someone had broken in and burglarized your home. You ask your spouse to call the police and direct your children to stay outside the house. But what do you do next? Would you assume your best impression of Sherlock Holmes, grab a magnifying glass and immediately start investigating to determine who the burglar was? Or would you instead take stock of your house, determine what valuables were missing, and figure out how the burglar got into the house and the alarm system was not triggered?

The average person would not devote his or her time and energy to finding the suspect and would leave that to the people who are trained in that field, law enforcement. Instead, most people would focus on recovering from the burglary. They would restore the house, determine what was destroyed or stolen, and file insurance claims for the stolen property. They would then focus on how the burglar got into the house. Was the alarm set? Were all the doors and windows locked? Was a family friend supposed to stop by every couple of days and check on the house? Then, after understanding how the burglary occurred, they would hopefully take steps and precautions to make sure that a similar burglary could not happen again.

We don’t focus on discovering the burglary because we, as private citizens, need to get back to our everyday lives as quickly as possible. We do not focus our energy on discovering the identity of the burglar because we know that we have police officers and detectives who are trained experts to figure that out.

So why should we treat cybersecurity attacks and data breaches any different?

In June 2017, the Ponemon Institute released its annual Cost of Data Breach Study. The report underscores that a company’s failure to recover from a cybersecurity incident quickly and efficiently can increase damages and costs. According to the report, within the United States, the average cost for each lost or stolen record containing sensitive and confidential information is $225. The average total cost for organizations that participated in the study was $7.35 million.

The Ponemon Institute also reported that the time that it takes for a company to identify and contain data breaches affects the total cost of the data breach. If it took less than 30 days for a company to contain a data breach, the cost to contain the breach was $5.87 million. If it took 30 days or longer to contain the breach, then the cost increased to $8.83 million. Additionally, data breaches caused by malicious or criminal attacks took the longest for a company to detect and contain, at an average of 303 days to identify and contain.

The report also highlights the hidden costs of a data breach, the internal resources that companies use to deal with a data breach. This includes the time employees spend on investigations of the incident or data breach notification efforts, as well as loss of brand value and reputation and customer churn. In 2017, of the $225 average cost for each lost or stolen record, $79 was attributed to indirect costs.

The Ponemon Institute’s annual report demonstrates that focusing on attribution after suffering a data breach is a waste of time, money and other resources. Law enforcement have both the training, resources and experience to identify the actors responsible for cybersecurity incidents and data breaches that companies simply don’t have. Additionally, identifying the actor responsible for the cybersecurity incident does not help the company recover from the attack. Knowing who was responsible for the data breach will not help the company get back to day-to-day operations. Companies should focus on containment of the cybersecurity incident, restoring any impacted operations as quickly as possible, and preventing a similar cybersecurity incident from occurring in the future. Rather than answering the whodunit, companies should get answers to the following questions, retaining a forensic expert if necessary:

- What systems and information were accessed or acquired?
- Was the security, confidentiality or integrity of any information impacted?
- What controls were in place prior to the incident?
- What controls failed?
- How did the controls fail?
- How can we restore our systems and any information that was compromised?
- Do we need to notify consumers and any government agencies?
- What controls should be updated, replaced or changed to prevent this incident, or a similar incident, from occurring again.
- Is there a third-party vendor, or some other party who may be liable for the breach? If so, should we file a legal claim?
- Do we have cyber insurance? If so, is there is a dispute over the coverage?

Handling the legal fallout from a data breach is an important aspect of recovery that can get lost when a company devotes too many resources to attribution.

Companies should consider using arbitration or mediation to resolve data-breach-related disputes, as they allow for the dispute to be confidential and, with the right arbitrator or mediator, can save the parties significant time and money.

The key is using an arbitrator or mediator who understands the technology and the law. The arbitrator or mediator can then cut to heart of the technical and legal issues at play to resolve the dispute efficiently and help the company stay on the path to remediation.

By directing their energy towards identifying and recovering from a cybersecurity incident, companies can mitigate the amount of time, money and resources needed to recover from a breach.

DANIEL GARRIE is an arbitrator, forensic neutral and technical special master at JAMS. He is executive managing partner of Law & Forensics LLC, and head of its computer forensics and cybersecurity practice groups. He is also the CISO at Zeichner Ellman & Krause LLP.

MICHAEL MANN is a senior legal analyst at Law & Forensics LLC where he works in the e-discovery and digital forensics practice groups.