integreon

The Challenge of Cyber Incident Response - Beat the Clock, with Accuracy

Thursday | October 24, 2019
by **Joanne Shields**, Director, Integreon

Once a company recognizes it had a cyber incident, the clock starts and it's a rather unforgiving taskmaster.

The insurance companies, law firms and cyber/computer forensics consultants retained to assist compromised entities often have as little as 45 days to notify affected people about the incident. If really in a pinch, a short extension can be requested in court, but it's still not a lot of time, especially when dealing with thousands of affected records. Fully responding within this timeframe is a tall order, given that each person whose data was impacted may have had a different mixture of personal identification and health data exposed by the incident.

Forensics firms, insurance companies and computer forensics consultants enlist the help of digital or "cyber" detectives to investigate a cyber incident and determine its scope and those potentially impacted. The point of this investigation is to discover if a breach occurred, but also to find out whose data may have been exposed in order to compile a consolidated entity list and notify impacted parties. Failing to make notification within the time allotted can lead to fines and other penalties, not to mention exposure to reputational risk.

> ***Cyber incident response (CIR) data review is often compared to litigation document review, but these processes differ in many fundamental ways.***

These consolidated entity lists must be accurate, comprehensive and rapidly generated which calls for quick ramp-up, exceptional planning, experience and seamless execution. The need for speed cannot be prioritized over the importance of accuracy when building a list - both are equally crucial. Done right, cyber incident response teams can build lists quickly to meet pressing deadlines, successfully overcoming obstacles that arise along the way. This requires a well-planned orchestration of the right resources, process and technology.

Cyber incident response (CIR) data review is often compared to litigation document review, but these processes differ in many fundamental ways. Lawyers reviewing documents for litigation or compliance are typically reading through documents and emails, tagging items which are relevant to the matter at hand. On the contrary, CIR professionals must be highly analytical, approaching their data review process like detectives searching for lost objects and identifying specific owners of those objects.

From a data perspective, each cyber incident has a unique set of circumstances. At the outset of a cyber incident response project, those responsible for creating a consolidated entity list must educate themselves on the nature of the documents they are investigating and learn about their origin, purpose, meaning, associated jargon, and industry acronyms. These projects must be handled carefully, with informed professionals poring over the data.

For example, if the compromised organization was a hospital, both health information and personal ID information would most likely be at risk of exposure. Patient information pertaining to diagnoses, health insurance IDs, medications and date of birth could be included in the examined data set. If the breach impacted a clothing retailer's customers, list development teams could be looking for credit card numbers, addresses and phone numbers. A government agency cyber incident may expose driver's license or passport numbers, criminal records, or social security numbers.

Cultural and linguistic quirks like nicknames can pose challenges for CIR data analysts. The English language is famous for its plethora of nicknames. A man named Robert J. Smith may be called "Bob", "Bobby", "Rob", "RJ" and more. He may sometimes use his middle initial to identify himself, and sometimes not. The job of the analyst is to determine whether all these aliases refer to the same individual, so that person can be notified of all data exposures which pertained to him. If a reviewer mistakenly creates two entries with the same name, the organization relying on their work product will be understandably upset. These duplication errors must be avoided at all costs with assistance from human due diligence and technology tools.

Nickname and middle initial variations are two of many potential pitfalls that can thwart construction of a clean notification list. Typos and misspellings such as "Brain" instead of "Brian" or lack of a middle initial can be reconciled by using pivot tables in Excel. Pivot tables allow reviewers to query data entered into Excel, using a unique identifier like a social security number to determine if duplicate entries have been made. Hidden columns or rows in Excel can also conceal data that needs to be examined, so the examiner must look closely to detect even the invisible. Driven by rigorous standards, consolidated entity list development teams will generally run at least 40 standard searches that are checked for misses and cleared every day.

Recently introduced data privacy regulations like GDPR have added a level of complexity to CIR work. Since GDPR protects more types of data, there are more incidents, resulting in more notifications taking place. *For example, GDPR protects mobile telephone numbers. Imagine how many people include their mobile numbers in their email signatures, meaning that if their email messages are exposed, each message's email signature with a mobile number must be identified and extracted for notification.*

GDPR also protects personal information, mentions of which may be woven through records and correspondence. Due to GDPR regulations and also their Canadian equivalent PIPEDA, CIR professionals must add searches to find types of information that compliance earmarks, including personal signatures, marital status, race/ethnicity or sexual orientation, which are all considered private.

The United States does not have a national GDPR equivalent yet, though some States have put forth their own data privacy rules and regulations. **The California Consumer Privacy Act (CCPA) passed in June 2018 sets forth a stringent set of data privacy guidelines with an imminent compliance deadline of January 1, 2020. Some other states are mobilizing to establish their own privacy protections as well.** Certainly, California's strict approach sets a strong first example of what's to come for other states.

> ***Technology tools are used throughout the CIR process, but the process cannot be fully automated without human leadership and analysis.***

Technology tools are used throughout the CIR process, but the process cannot be fully automated without human leadership and analysis. Electronic discovery and document review software can be reverse engineered to assist CIR notification and tools specifically for cyber incident use have recently emerged and are gaining traction fast. However, technology tools alone cannot reliably determine if the information is or is not deemed provide based on the various applicable laws.

For example, if you searched for the word "Medicare" on documents coming out of a human resources breach that had paycheck stubs, almost all of these hits would be FALSE or not applicable. This is because the Medicare mentions are mostly attributed to Medicare fees being deducted from everyone's paycheck, not indicating that the individual has Medicare as his or her primary insurance provider. In most cases, employees do not have Medicare based on the fact that they are still working. However, if your data set comes from a compromised health services provider, you will get many TRUE or positive hits on Medicare because Medicare is the patient's insurance provider. There are hundreds of other examples like this which make human judgment incredibly important in the cyber consolidated entity list development and notification process.

Cyber incidents are definitely on the rise, and companies must face the fact that they may be impacted more than once, perhaps multiple times. Computer forensics and cybersecurity consultants, law firms and insurance companies assisting these clients must include acumen for consolidated entity lists into their overall response process, whether they provide these services themselves or bring in a qualified partner. Those who do this work must be experienced at diving in and building lists quickly, sometimes maintaining 24/7 schedules across the globe to ensure quality work done, on time. Once begun, the cyber clock stops for no one, so CIR teams must beat the clock and deliver the consolidated entity list without fail, every time.

About the Author

Joanne Shields is a Director at Integreon, a global alternative legal service provider (ALSP). An attorney with deep experience with data and document review, Shields leads data review teams for Integreon's Cyber Incident Response (CIR) service group at the company's service delivery center in Noida, India.