The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

October 2013 Volume 21, No. 10

What Is Remediation?

*The Editor interviews **Antonio Rega**, Managing Director in the Technology practice, FTI Consulting.*

Editor: Tell us about your background and current role at FTI Technology.

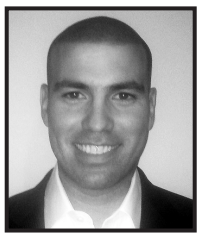
Rega: I'm a managing director in the New York office and have been with FTI since 2005. Part of my duties and responsibilities include managing and overseeing initial e-discovery efforts including collections, preservations, litigation readiness and other related matters involving risk management. I handle a wide range of high-profile computer forensic investigations and have provided sworn testimony on matters relating to computer forensics and e-discovery.

Editor: We're hearing more about a process called remediation. What is "remediation" and how does it relate to e-discovery?

Rega: Put simply, data remediation is securely removing and destroying data. Many of the techniques and tools are similar to those used for forensic investigations or collection as part of an e-discovery process. And, it is an increasingly important information governance measure that companies are incorporating to manage data retention.

Editor: What are some of the common scenarios for the use of remediation?

Rega: Readers will likely be familiar with some of the more common use cases, such as securely removing old and unused legacy data systems, or eliminating personally identifiable information (PII) within company archives. Another scenario that may not be as obvious, but is certainly a frequent request, is to manage data when employees leave companies within industries with a lot of intellectual property (IP), such as biotech. Upon the departure of any given employee, there is often a focused remediation process whereby the outgoing employee's work product is securely deleted and removed from his machines. For these matters, there is often an initial exit interview with counsel present to help identify the documents to remove from his systems.



Antonio Rega

Another type of remediation scenario occurs when two companies in a partnership are separating. As part of the remediation process we can identify IP-related documents that Company A needs to have removed from its systems. Sometimes that also includes providing a copy of those identified IP documents to Company B. Again, that is a process that often includes working with counsel to identify documents for remediation and ensure all necessary steps are taken to securely delete or transfer the documents of interest.

As another example, we were recently involved in a matter for a healthcare company that had stored sensitive credit card information for hundreds of patients. In order to be in compliance with payment card industry (PCI) requirements, the company needed to conduct a large-scale remediation of that data. The data was housed within a number of different source-media locations: network servers, file servers and desktop computers. The large number of custodians involved, combined with HIPAA data privacy and security concerns, required that we conduct the remediation within their environment while utilizing our own software and hardware tools. The remediation process included applying PCI-compliant search patterns across the data sets. Statistically valid samples of data were pulled to ensure all of the credit card data was captured. As items containing credit card information were identified, a dynamic reporting functionality was generated to review the flagged contents. This provided the option of conducting a small-scale review of the flagged items as an added layer of confirmation. From there, once items were confirmed for remediation, proprietary deletion scripts were implemented across the network, and log files detailed the items remediated.

I should note a few areas of additional complexity. Some items could potentially fall within a litigation hold, so instead of securely deleting them, we quarantined them in a secure location. Additionally, because we were focusing on active content, we recommended certain internal controls to be put in place to ensure that users could not recover archived or deleted content. The remediation process was focused on active content that users would readily be able to access as opposed to any legacy-related and/or archived content.

Editor: In the first instance when an employee leaves and there is not a non-compete, is there any way the employer can possibly prevent him from using those documents?

Rega: Much of it will depend on whether a company has internal controls in place. Typically, an outgoing employee will be asked to sign forms confirming that he or she has not taken any such documents. For companies that do not have strict controls in place, or in cases with extenuating

Please email the interviewee at antonio.rega@fticonsulting.com with questions about this interview.

circumstances, they may want to take an additional step to ensure there have not been any data breaches. In this instance, they often rely on an outside consultant to perform that work. Ideally, internal controls should be implemented to preclude the need for remediation.

These internal controls are often a crucial element not only in information governance but the litigation readiness process in general. It is also a cost-saving measure.

Recently, we had a scenario where two high-tech companies were separating from their partnership. FTI worked with internal counsel from both companies to develop and implement an action plan for identifying data for remediation. Prior to any actions, the parties agreed to generate copies of interest to the other party, then deleted those documents from the other entity's equipment. Once that process was complete, we drafted a certification that basically outlined the methodologies and steps performed, underscoring those were performed with accuracy and completeness.

Editor: Is it common to provide certifications on the process?

Rega: It is certainly common for remediation projects in which outside auditors are involved. In such instances, the certification process becomes paramount because companies want to ensure that their process can hold up in court. Even when both parties are in agreement and acting in good faith, a certification can provide an added layer of comfort that the process was done in a complete and thorough fashion.

Editor: How are you able to ensure that all of the file content is deleted?

Rega: There are certain tools that will calculate where the document has resided in its active state on the hard drive, and forensic and remediation experts can work to ensure that important technical matters, including data remnants, are addressed. For example, in a Windows Operating System environment, when a document is deleted, the operating system does not actually delete the document, but places a character in front of the document name, rendering the previously occupied space available for the operating system to allocate as needed. The so-called document still resides there in its fully intact state until another document takes its place in that space. In our case the deletion is twofold: not only do we delete the document itself but any residual remnants as well.

Editor: Can you give an example of how remediation is used to control the spread of IP?

Rega: One recent scenario involved the departure of outgoing employees from a technology firm. It required content deletion from the host computers in the presence of an attorney for each employee. We interviewed the departing employees, in the presence of their attorneys, to identify certain locations where specific documents resided. Once all sides agreed on the documents for deletion, we captured and remediated the designated documents and made sure there weren't any fragments of the document to be recovered. At the conclusion of that process, we developed a detailed affidavit that outlined step by step the measures we implemented as well as assurances that the process was complete and thorough. The challenge in this undertaking was that there were a couple of different parties involved at each location, and there were numerous times when we had to deploy a team to perform the work. There was quite a bit of nuance involved in the questions asked and in the identification of those documents in order to reach agreement that those were indeed documents that needed to be remediated.

Editor: What are important considerations for a legal team or client in handling a matter that involves remediation?

Rega: It's important to identify any items that may be within a litigation hold as those items can't simply be deleted or remediated. Also, legal teams need to work closely with the IT team to understand what data is no longer necessary within legacy systems. As mentioned earlier, this can help save costs and also reduce cybersecurity risks.

Also, teams should assess the internal controls in place prior to undertaking any large or even medium-scale remediation. This is because the company may already have controls in place to manage and/or purge legacy data. Any of the above examples are proactive measures that can be taken in advance of any remediation steps that can assist in mitigating the overall scope of a remediation process.

"Depending on the type of remediation that is involved and the specifics of the engagement, there are certainly scenarios where IT can perform at least a subset – or more – of the tasks with minimal guidance from a third-party consultant."

Editor: Are there scenarios when an in-house IT should perform a remediation without third-party assistance?

Rega: Depending on the type of remediation that is involved and the specifics of the engagement, there are certainly scenarios where IT can perform at least a subset – or more – of the tasks with minimal guidance from a third-party consultant. This determination is primarily dictated by the amount of experience internal IT may have with the remediation process or e-discovery procedures in general, such as preservation of metadata and secure deletion of content. To the extent IT may not be as well-versed in these processes, a consulting firm like FTI can help provide guidance and/or perform some or all of the action items involved. This third-party validation can be especially helpful in litigious or regulatory scenarios.