Environmental

VESTIGE Digital Investigations

Sample Cases

The following descriptions highlight a variety of Environmental matters which benefitted from involving Digital Forensic and Cybersecurity Experts both reactively and proactively.

Plant Explosion | Digital Forensic Preservation

A major chemical company suffered a plant explosion. In addition to multiple fatalities, there was an airborne release of potentially harmful chemicals threatening individuals in area homes. Vestige was engaged to accompany the legal team in interviewing senior management and first responder personnel. Vestige conducted an immediate collection of data from multiple forms of devices including phones, tablets, computers and social media. This was complicated by the company's Bring Your Own Device(BYOD) policy which merged personal and professional data.

The onsite preservation efforts enhanced our clients (Law Firm) ability to represent their client and guide the response efforts and media coverage. The presence of Vestige assured that the data was preserved properly and quickly made available for counsel to review and react.

Air Testing Equipment | Forensic Evaluation

A chemical company employee suffered injuries by breathing harmful air. The company had never experienced an emergency of this type and the air testing equipment did not sound an alarm. Upon further investigation of the settings of the air testing system, it was determined that the levels of permitted chemicals had been increased by three times.

Vestige was contacted to evaluate the on-premesis air testing device to determine if it was changed in any way. Upon completion of testing, Vestige determined that the detection settings of the device were altered allowing three times the rate of harmful air contents than the device was originally set to detect. Vestige went a step further and through a review of deleted data from the device and security camera's in the area, was able to determine the time and identity of the individual who made the unauthroized changes to the air testing system.

Water Testing | Forensic Evaluation

A regional water authority was sued over claims of poor water quality. One of the terms of settlement of the matter required the water authority to provide results of water testing for three years to the environmental group responsible for monitoring. The water authority complied with the terms for the first year then stopped sending results. Upon request, the monitoring group was told the testing results were lost through a system malfunction and could not be recovered. Vestige was brought in by the monitoring group to determine if the testing results could be recovered. Vestige determined the best way to begin the investigation was to image the computer which housed the database that stored the testing results and forensically search for them. With a minimum cost of time, Vestige was able to recover the lost test results in a deleted version of the testing database and provide them to the monitoring group.

Responding to Government Enforcement Actions | Forensics & Consulting

The Environmental Protection Agency started a formal investigation against a US-based hyrdofracking company after a whistleblower from the company provided information about the manner in which the fracking by-products were being treated and discarded. The case alleged that after-hours workers from the company were discharging waste from the drilling mud, slurries and other fluids used in fracking into retaining ponds around the company's headquarters in order to avoid costs associated with appropriately processing the discharge prior to reintroducing to the environment. A criminal inquiry into who at the company was aware of these activities and potentially directing the activity hinged upon the analysis of the organization's internal e-mail systems, text messages on management and supervisor's mobile phones as well as Internet searches conducted on company-owned laptops. The National Enforcement Investigations Center (NEIC) – the EPA's internal digital forensic unit was involved. The organization's systems were seized, including personal devices of the company's owners. Private digital forensic analysis worked with the defendant's (company and owners) legal team to:

- Negotiate obtaining forensic images from the EPA to conduct analysis over the company's seized assets to anlyze the fact pattern mount a defense,
- Helped the legal team obtain and navigate a list of particulars to determine the scope of the government's knowledge of the situation,
- Assisted the legal team to put its own document requests together.

In addition, digital forensics could be used to:

- Conduct an internal investigation at the direction of the Board of Directors, the outside legal team, company management, etc., to understand the depth of the knowledge of any wrong-doing,
- Assist with determining whether enforcement's electronic evidence discovery requests are overburdensome,
- Provide testimony on the findings, including affidavit, deposition and hearing or trial testimony,
- Assistance during sentencing phase to provide mitigating factors (including highlighting "Brady Material") that might drive a plea bargain or shorter sentence/lesser fine.

Industrial Controls at Municipal Utilities | Cyber Readiness Assessment

A local municipality spun off its utilities (power, sewer, water) into a stand-alone, quasi-private/governmental entity. While the utility purchases 90% of its power through other providers, it still is responsible for and runs a coal-powered 80-megawatt power plant as part of its energy diverse portfolio. The entity is 100% responsible for distribution of the energy delivered by its portfolio offerings. In addition the entity runs the sewer/sanitation and water treatment plant. As the entity is in the crosshairs of the rural area's critical infrastructure, the Board of Directors and Management had continued concerns about CyberSecurity and the manner in which an outside attacker could affect any of these systems. Power distribution and the operation of the power plant resided on one particular Industrial Control System (ICS), while the water treatment and sanitation was controlled through a different ICS. The municipality turned to Vestige as a provider that not only understands the proactive side of CyberSecurity but also has involvement in thousands of data breaches and compromises so we understand the manner in which systems have been affected.

continued

Involvement included:

- Providing a comprehensive assessment of the organization's CyberSecurity Readiness,
- Assistance with creating a Written Information Security Plan (WISP) that addresses the policies and procedures they need to have in place from a proactive standpoint,
- Assist the organization develop a CyberSecurity Incident Response Plan (IRP) and to incorporate that IRP into their overall Crises Response plans.

Thankfully, our involvement has not been on the reactive side of CyberSecurity, but in the event of a security incident, we could also:

- Investigate an incident, identify how it occurred, understand the scope of the breach, help to remediate the matter and assist in determining notification requirements, mitigate, respond and recover from a breach.

Merger & Acquisition | Cyber Due Diligence

As more and more organizations consider transactions (M&A) as a means of expanding, increased attention to CyberSecurity during the due diligence phase is not only becoming more popular, but is becoming a must. The old adage in the CyberSecurity world is that there are two types of companies – those that have been breached & those that have been breached and know about it! Too often, purchasers don't know or understand the full liability of a potential data breach until many months or even years after closing a deal. World-wide, non-industry-specific, the average time that an attacker goes unnoticed within an environment is roughly 270 days. While not specific to Environmental organizations, any and all Merger & Acquisition candidates should undergo a CyberReadiness Assessment during the due diligence process prior to close. Vestige performs these kinds of assessments in due diligence all of the time. Recently we conducted such an assessment for a public company acquiring a service provider. Beyond revealing that the selling entity had experienced a very minor compromise of Personally Identifiable Information (PII) approximately 3 years prior, our assessment also revealed approximately 20 areas of concern and provided explicit instructions as to how these should be remediated. It gave a game plan for what steps the purchasing entity needed to take during the first several days after closing to ensure that the environment was as secure as possible. During the 2 months that elapsed between our assessment and the closing date, the selling entity was hit with a Ransomware attack. The purchaser called us back in to:

- Identify how the compromise occurred,
- The scope of the compromise,
- Determine if any sensitive data was compromised or leaked from the organization,
- Assist legal counsel with whether notification duties were triggered,
- Determine what needed to be accomplished to isolate and mitigate the compromise.

Upon investigating we determined that the compromise occurred due to a trusted 3rd party connection with a supplier of the service provider. This was detailed in our initial assessment, accompanied by a warning that it was a back door into the environment and something which the purchaser would definitely want to eliminate as soon as the deal was closed.