November 16, 2011

Temple University Open House

Forensic Technology Solutions

pwc

Temple Open House
Agenda

1. About the Presenter

- Education / Employment
- How did I get into this type of work?

2. Forensic Technology Solutions

- What We Do
- FTS Engagement Experiences

3. Real World Experiences

- Global ATM Fraud Investigation & Remediation
- Payment Card Data Breach & Malware Response

4. Q & A

About the Presenter

The Presenter

- Mark LeMay
- Been working at PricewaterhouseCoopers (PwC) for 5+ years

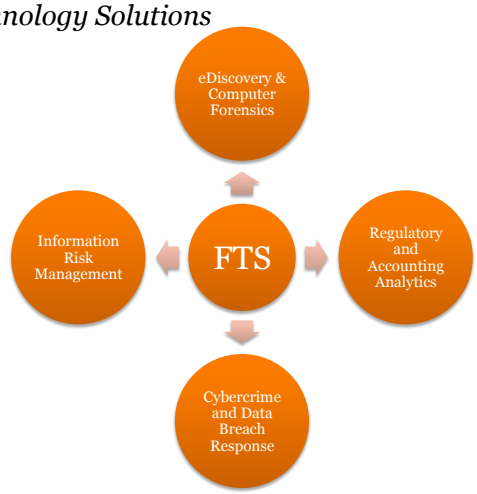
Education / Certifications

- Master & Bachelor of Science in IST from Drexel University
  - Concentration: Database Administration
- Certified Fraud Examiner (CFE)
- Oracle PL/SQL Certified Associate (OCA)

Experiences

- How did I get involved with this type of work?

What We Do
Forensic Technology Solutions



What We Do
FTS: eDiscovery & Computer Forensics

What We Do	Data Sources	Tools We Use
• Hard Drive Imaging	• Laptops	• Encase, Paraben, Forensic Toolkit (FTK)
• Media Restoration	• Servers	• Stratify
• Forensic Image Analysis	• Backup Tapes	• Relativity
• Deleted File Recovery	• Flash Drives	• iConect
• Manage Document Reviews	• Smartphones, Cell Phones	• Trident
• Data Preservation	• Email Accounts	• dtSearch
• Legal Document Productions	• Loose media	• TrueCrypt
• Expert/Fact Witness	• Hard Copy/Paper Documents	• WinZip, WinRAR
		• UltraEdit

What We Do
FTS: Regulatory and Accounting Analytics

What We Do	Data Sources	Tools We Use
• Accounting & Tax Data Analytics	• Accounting Data (GL, AR, AP, Payroll, etc.)	• Oracle
• Regulatory & Compliance Reviews	• Sales & Subscriber Data	• Toad for Oracle
• Fraud, Risk & Controls	• Insurance Claims	• SQL Server Management Studio
• Transaction Monitoring	• Licensing/Royalty Data	• MS Office Suite
• License Management	• Bank Customer & Account Information	• VBA, VB Scripting
• Data Normalization & Matching - Names, Addresses, Currencies, Dates	• Credit Card Transactions	• PwC Tools (TRIA, GIR Tool, GL Tool, CaseIT)
• Ad Hoc Data Analytics - Identify Gaps, Patterns, Trends	• Employee, Vendor, and Customer Master Files	• UltraEdit
	• Watch Lists (World-Check, World Compliance)	• Visual Studio
	• Software Asset Management Tool Output	• Monarch
		• Command Line Batch Files

What We Do
FTS: Cybercrime and Data Breach Response

What We Do	Data Sources	Tools We Use
• Computer & network intrusions • Data Theft & Breaches • Cyber Sabotage/ Extortion • Computer Fraud & Abuse Investigations	• Laptops • Servers • Backup Tapes • Flash Drives • Smartphones, Cell Phones • Email Accounts • Loose media • Hard Copy/Paper Documents • Physical memory (RAM)	• Encase • Forensic Toolkit (FTK) • Helix • HBGary • F-Response

What We Do
FTS: Information Risk Management

What We Do	Data Sources	Tools We Use
• Discovery Readiness • Enterprise Content Management (ECM) • Records Retention Strategy • Data Privacy & Security	• Paper documents • User Files • Production databases • Email (desktop & server) • Server backups • Intellectual Property (IP) • Legal Contracts • Web Content/Multimedia (videos, audio, designs)	• MS Office Sharepoint • Symantec Vontu Data Loss Prevention • FileNet® Workplace • McLaren™ Enterprise Engineer • Custom policies and procedures (e.g. Data retention policy) • Custom templates/style sheets • Custom tools

FTS Engagement Experiences
Types of FTS Engagements

Investigations	•Embezzlement/Typical Fraud Case •Foreign Corrupt Practices Act (FCPA) •Anti-Money Laundering (AML) •Disaster Recovery •Intellectual Property Disputes •Ponzi Scheme •Cybercrime/Data Breach Response
Compliance / Audit	•Financial Statement Validation (CAAT) •Regulatory Compliance & Reporting (IRS, SEC) •3rd Party Due Diligence •License Compliance & Software Asset Mgmt. •Know Your Customer (KYC)
Process Improvement	•Business Processes Optimization/Remediation •Information/Records Management

Real World Experiences
Global ATM Fraud Investigation & Remediation

Business challenges

- A data breach occurred at a global electronic payments processor and credit card issuer resulting in the fraudulent disbursement of millions of dollars and compromise of tens of millions of credit card numbers, SSN, and other Personally Identifiable Information (PII) and Payment Card Industry (PCI) information.
- The client needed assistance understanding the location and current state of the PII and PCI data elements on their systems so that they could meet statutory notification requirements, and meet PCI Data Security Standard (PCI DSS) requirements regarding the storage of card holder data.
- The client also needed assistance remediating their systems of the sensitive data elements identified, as well as their policies and procedures, so that they could reduce their overall security and compliance risk.

Approach

- PwC performed an assessment of the client's infrastructure and current state of the PII and PCI and provided remediation services. PwC utilized a Top-Down approach to understand known risk areas and a Bottom-Up approach by conducting Nmap scans, schema extracts, field name scans and data validation procedures to identify previously unknown risk areas, as well as validate management assumptions gained from the Top-Down approach.
- PwC performed data discovery services for compliance with statutory laws requiring notification of affected people and for compliance with PCI DSS standards.
- PwC then drafted policies and procedures that increased compliance with respective legal, regulatory and contractual obligations, and decreased data privacy and security risks. PwC also provided the client with a High Risk Data Discovery Summary Tool.

Results

- The client was able to gain a better understanding of not only the location and current state of the sensitive data elements within their systems, but also better manage the legal, regulatory and contractual obligations with regard to the high risk data.
- The client was able to implement a streamlined approach, isolating specific data such as PII and card holder data, as necessary, in order to identify those components that needed protection beyond the newly developed policies and procedures.
- Ultimately, the client was able to secure its most sensitive data in a systematic fashion, comply with data breach notification requirements and also regain its PCI DSS compliance.

Real World Experiences
Payment Card Data Breach & Malware Response

Business challenges

- The client, a Fortune Global 500 company, experienced a data breach of over 4 million credit and debit card numbers from their systems, resulting in over 2,000 known cases of fraud. As a result of the data breach from 2 years prior, the client was subjected to an ongoing investigation by the Federal Trade Commission (FTC).
- Working in conjunction with the client's outside counsel, PwC assessed the company's data security practices against the standards set forth in prior FTC data breach consent decrees to help the client meet compliance obligations

Approach

- After selecting the assessment criterion, PwC implemented a series of workstreams to review and benchmark the current state of the company's IT security.
- This review was performed against a recognized security program framework, International Organization for Standardization / International Electrotechnical Commission 27002:2005.
- PwC searched for Sensitive Personal Information, Payment Cardholder Information and Personal Health Information by leveraging tools owned by the client (Guardium and Vontu).
- PwC leveraged custom regular expressions and other proprietary search/validation techniques to compliment these tools in order to minimize false-positive results and reduce manual review time.
- PwC assisted with the development of long term policies, processes and procedures to deploy a sustainable program leveraging the tools and technologies utilized during the initial discovery phase.

Results

- The company's information security program was neither comprehensive nor sustainable, and did not meet the requirements of an FTC consent decree. PwC observed weaknesses across all control objectives, including a number of technical deficiencies. In addition, PwC noticed a significant disconnect between the level of security expected by senior management and the actual operational practices.
- PwC worked with the client's outside counsel to develop a series of remediation activities bundled into a comprehensive high priority program focusing on addressing high priority reactive issues, as well as creating a sustainable program and culture to remediate security issues on an ongoing basis.

The End

Questions?

Contact Information

Mark LeMay
Email: mark.lemay@us.pwc.com
Office: 267-330-2031