

# *Case studies*

PwC Cybercrime  
US Center of Excellence  
Advisory - Forensics

# State sponsored network intrusion

## Act of economic espionage

### Client issue

An international energy company headquartered in the US was contacted by the FBI and advised that their network had been compromised by a state sponsor. A foreign government was actively infiltrating the company's network and systems. The FBI offered to share information with onsite individuals holding a US Government Top Secret clearance. As a result, the company hired PwC's cleared cybercrime team.

The state sponsor leveraged an Advanced and Persistent Network Intrusion to compromise hundreds of geographically dispersed systems to steal economic intelligence from the company related to a myriad of business deals.

### PwC actions

#### Computer forensics

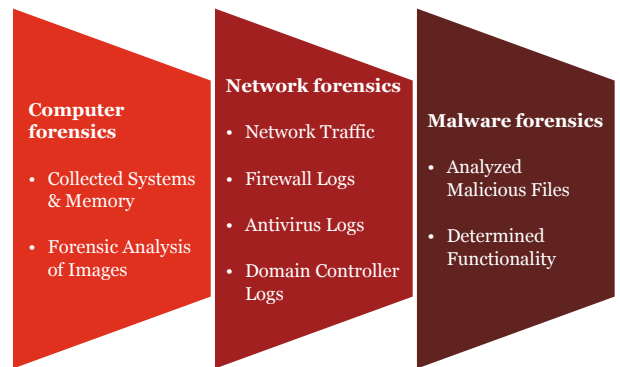
The perpetrators compromised hundreds of systems across a geographically dispersed area, including the United States, Middle East and South America. PwC worked with the client to identify those systems and forensically analyze them.

#### Network forensics

PwC collected log data from a range of client systems in order to perform network forensics. This analysis aimed to identify patterns in the compromised network communications.

#### Malware forensics

PwC's in house malware lab was used to analyze suspected malicious files and processes found on the systems. This analysis determined the functionality and identified the types of incoming and outgoing communications associated with the malware.



### Findings

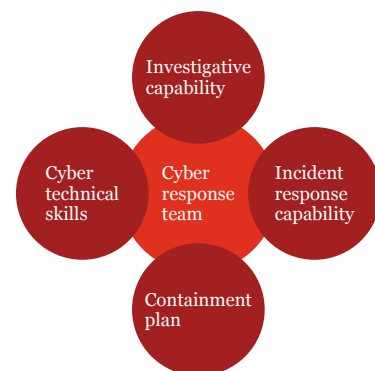
PwC's cyber forensics resulted in the following key findings:

- Identified the **access methodology**
- Identified the methods for **moving through the environment**
- Confirmed the **data theft of economic value**
- Identified method of **exfiltrating data from the environment**
- Confirmed the method in which the state sponsor stole **domain administrator passwords**
- Identified the attacker's **persistent remote access** to the company's network environment
- Determined the attackers had **access to the client's environment for at least 2 years.**

### Remedial actions

PwC helped the client develop an internal Cyber Incident Response Team to respond to future advance cyber intrusions. The development of this team focused on the following cyber response capabilities:

- **Incident response capabilities** – Developing a customized internal Incident Response capability for the client to investigate advanced cyber incidents.
- **Investigative capabilities** – Identifying technical and human resources to deploy to respond to both an internal or external cyber crime incident.
- **Containment plan** – Development of a consistent approach to contain an advanced cyber threat.



# Global ATM fraud

## Network intrusion, PCI data theft, & PII exposure

### Client issues

A Global Fortune 100 company experienced a cyber attack and data breach resulting in the loss of Personally Identifiable Information (PII) for millions of customers. During the cyber attack, debit card numbers and their associated pin numbers were breached. The perpetrators used this information to create phony ATM cards with the stolen data embedded on the cards. The hackers distributed the fraudulent ATM cards to individuals located in dozens of cities throughout the world. In a coordinated effort, the money mules used the ATM cards to withdraw several million dollars in cash very quickly.

### PwC actions

#### Computer forensics

PwC forensically preserved hundreds of systems to support investigative needs and position the client to prepare for legal and regulatory actions. PwC forensic technologists worked closely with information security Subject Matter Specialists to forensically analyze the collected images.

#### Network and malware forensics

PwC's initial incident response identified the root cause of the network intrusion. Further, PwC identified all compromised systems in the environment and multiple hostile remote access capabilities. This involved analysis of discovered custom malware and network traffic and logs. The Security team also helped implement a more detailed review through penetration testing of the Company's corporate network.

#### Protected data analysis

PwC analyzed both structured and unstructured data stored on compromised systems for PII and PCI data. After identifying data sources containing PII, PwC consolidated, de-duplicated and organized the unique instances of the information.

#### Disclosure preparation

PwC worked closely with the client's Office of General Counsel and outside counsel and a third party credit monitoring company to support a Breach Notification exercise.



### Findings

PwC's was able to identify and target the network intrusion, data theft, and lack of security protocols that resulted in the data breach by way of:

- **Computer Forensics** – PwC preserved and analyzed hundreds of compromised systems. The forensic analysis identified the initial point of intrusion, which systems had been compromised, and the how/where of undetected data exfiltration.
- **Malware Forensics** – Twelve custom malware instances were discovered and analyzed to determine purpose, functionality and capability. This malware was unknown and undetected by anti-virus technology.
- **Data Discovery & Disclosure** – PwC acquired and analyzed nearly 20 terabytes of data in order to identify sensitive customer data for notification.

### Remedial actions

After the initial incident response and forensic investigation, PwC conducted an independent cyber security assessment to support regulatory inquiries and remediation security weaknesses, assisted the client with becoming PCI compliance, acted as the client's interface to law enforcement. The latter involved the PwC investigative leader being interviewed by the Russian Federal Security Service in support of arrests and prosecutions in Russia.



# Fraudulent ACH transfers via online financial website

## Account takeover fraud

### Client issues

A Fortune 500 wealth management company noticed a spike in the reported instances of online fraud related to retirement savings plans. There were several reported incidents of Account Take Over resulting in loans against retirement savings accounts. The amount of the loan was then wired to a third party bank account unbeknownst to the account holder. The perpetrators were able to socially engineer their way to attaining customers login credentials by using phishing and spear phishing schemes.

### PwC actions

#### Computer forensics

PwC collected and preserved all digital evidence related to the incident. In total, PwC collected over 10 terabytes of digital evidence, including:

- Web Server Logs
- Windows Event Logs
- Firewall Logs
- Intrusion Detection System Logs
- Application Logs
- DB2 Audit Logs

#### Breach indicator assessment

PwC applied its proprietary breach indicator assessment to analyze the client's 30,000 node IT environment. This analysis included a two tiered risk based approach:

1. Reviewed all live, external facing web servers to determine if there were any breach indicators on those systems.
2. Reviewed all user workstations for same.

#### Log analysis

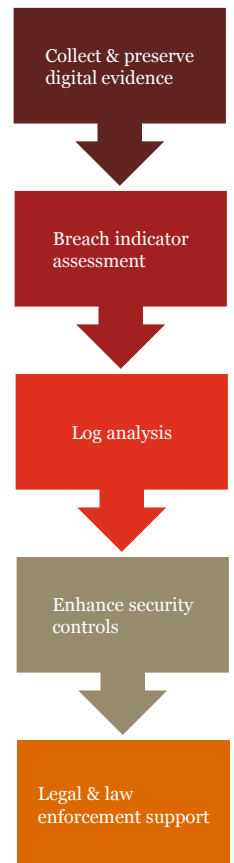
To determine the cyber behavioral characteristics of the online fraudster, PwC used its proprietary OBAT (Online Behavior Analysis Tool) to analyze certain log data. In effect, this helped determine what IP addresses and browsers the criminals used, and also identified what actions the criminals took after they illegally gained access to customer accounts.

#### Enhanced security controls

Based on findings from the cyber behavioral analysis, PwC was able to enhance security controls to prevent further online fraud.

#### Business impact analysis

Using the 10 terabytes of log data collected, PwC was able to identify the defrauded customer accounts and the cyber source of fraudulent access. This permitted the client to assess legal risk from a privacy breach notification standpoint and share invaluable evidence with law enforcement.



### Remedial actions

PwC worked with the client to implement a series of tactical changes to their IT environment while also implementing long term sustainable changes to help them more effectively identify and respond to cyber fraud.

Reactive

Sustainable

Application logic enhancements

Improved fraud monitoring technology

Network monitoring enhancements

In house incident response development

# Network intrusion

## Corporate servers used for spamming & DoS attacks

### Client issues

An Aerospace and Defense company was notified by an Internet Service Provider (ISP) that their computers were the source of a significant amount of spam being transmitted to one of the ISP's clients. The ISP provided a list of origin IP addresses for spam, which matched our client's internal IP address space. PwC was hired to investigate the issue and determine the validity of the allegation.

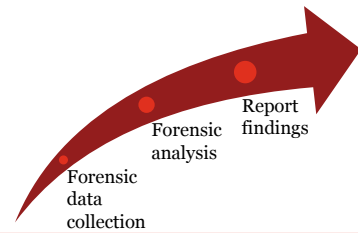
### PwC actions

#### Computer forensics

PwC forensically preserved a variety of computer systems based on the IP addresses provided by the ISP then analyzed those systems based on the allegations.

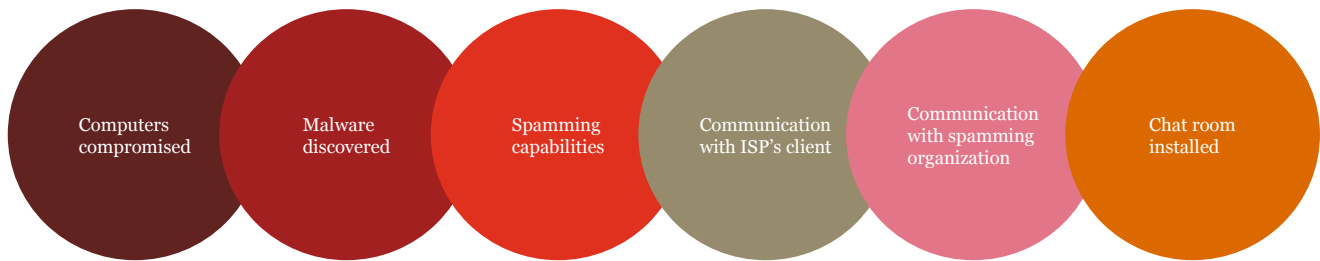
#### Malware forensics

Discovered malware was analyzed for purpose and functionality.



### Findings

- **Computers compromised** – PwC's analysis confirmed that our client's computers had been compromised.
- **Malware discovered** – Custom malware was discovered on the company's computers including spamming capabilities. Keystroke logging malware, used to log every user keystroke, was found on the company's computers.
- **Network connections to ISP's client** – Log analysis on compromised systems identified connections to the ISP's client.
- **Communication with spamming organization** – PwC identified transactions between the company's servers and the spamming organization.
- **Chat room installed** – PwC identified a chat room installed by the criminals. This chat room was used by the spamming organization to communicate.



### Remedial actions

The client used PwC's investigative findings to respond to the allegations by the Internet Service Provider. In addition, the company used this information to develop in-house containment and remediation activities with respect to the compromised systems.

# Cyber threat

## Imminent network threat reported by the FBI

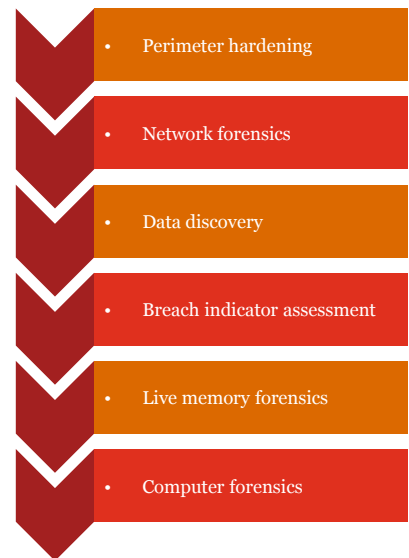
### Client issues

A financial services company was notified by the FBI that a cyber attack on their computer network was imminent and likely to occur within the next 48 hours. Computer systems contain payment card data, as well as other Personally Identifiable Information (PII) regarding the bank's customers, was stored and transmitted in the environment. The risks were varied: hackers accessing these systems and data have potential to engage in ATM fraud, wire transfer fraud, as well as identity theft, all with potential legal and regulatory implications on the financial institution.

### PwC actions

PwC quickly developed a series of risk-based actions to lockdown the client's IT infrastructure to help prevent a cyber attack. Simultaneously, PwC performed a breach indicator assessment to scan the IT network for malicious software and threats that could pose a threat to the company's network and data.

- **Perimeter Hardening** – PwC enhanced security and monitoring of Internet connectivity, user access controls and network/system logging.
- **Network Forensics** – PwC enhanced network monitoring for the company, collected network traffic and analyzed collected data for indicators of malicious activity.
- **Data Discovery** – PwC launched its proprietary data discovery methodology to determine the storage locations of data of interest to criminal attackers. This helped the client focus the investigation and its security enhancement efforts.
- **Breach Indicator Assessment** – PwC launched its proprietary methodology to investigate the company's internal cyber space for indicators of compromised systems.
- **Live Memory Forensics** – PwC preserved and analyzed volatile memory on systems it found that had indicators of malicious activity.
- **Computer Forensics** – PwC professionals forensically preserved and analyzed systems confirmed to have malware infections.

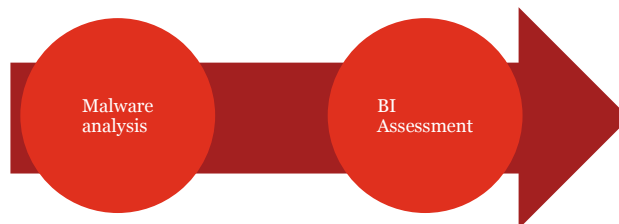


### Findings

PwC's breach indicator assessment identified hundreds of internal systems with Breach Indicators. PwC also identified previously undetected malware that had been installed on the company's systems nearly three years prior. PwC also identified the date of a mass data exfiltration.

### Remedial actions

Based on the Findings, PwC helped the client implement additional security measures to harden its IT environment and infrastructure.



# Corporate sabotage by IT executives

## The insider threat

### Client issues

The CEO of a consumer products company suspected disenchanted IT executives of exploiting their access to the company's private cyber space to engage in malicious activity. The company's private network stored credit card account data and other Personally Identifiable Information (PII) that could be used for malicious purposes if stolen. The IT executives had previously falsified written reports to internal auditors regarding a variety of mandated cyber security assessments. The CEO was concerned that the IT executives had established unauthorized remote access to the company network that would permit cyber sabotage upon termination of their employment.

### PwC actions

PwC implemented a series of reactive and proactive actions to help identify and contain any potential cyber security issues.

#### Forensic interviews

- PwC conducted forensic exit interviews of the terminated IT executives.

#### Computer forensics

- PwC preserved all computing devices of terminated employees and analyzed them for malicious activity.

#### Network forensics

- PwC collected network traffic and analyzed the data for indicators of malicious activity.

#### Vulnerabilities of external-facing systems

- PwC performed an Internet-born penetration to assess the feasibility of whether terminated employees could breach the perimeter.

#### Breach indicator assessment

- PwC launched its proprietary Breach Indicator Assessment to investigate internal cyber space for indicators of already compromised systems and in particular, malicious remote access capabilities.

#### Investigation of rogue wireless access points

- PwC swept the wireless access spectrum to identify unauthorized access points connected to the corporate network.

### Findings

PwC's actions helped identify two serious issues requiring immediate attention, as well as a series of security gaps in the company's infrastructure. A rogue, unauthorized wireless access point connected to the company network was discovered. This access point was configured to grant access to the company's private cyber space for the terminated IT executives. PwC's forensic analysis also identified multiple instances of malware on systems containing Intellectual Property.

### Remedial actions

PwC worked with the company to implement a two-tiered approach to remediate the identified threats and to enhance the company's security procedures and IT environment to help protect against a cyber attack.

- **Malware Analysis**  
PwC discovered and analyzed malware to determine its purpose, functionality and capability. The analysis was critical to making tactical security enhancements to the client's IT infrastructure and protecting Intellectual Property.
- **Perimeter Hardening**  
PwC enhanced security and monitoring of connectivity to the Internet as well as user access controls and network/system logging.

Malware analysis

Perimeter hardening

# Compromised of external-facing website

## Exposure of Personally Identifiable Information (PII)

### Client issues

A professional services organization was contracted by a Financial Institution to build a website hosting a survey for the Financial Institution. This survey collected Personally Identifiable Information (PII) provided by the bank's customers. The Financial Institution received a sudden uptick in complaints by banking customers that their identity had been stolen. This led the bank to suspect that the server hosting the survey had been compromised. PwC was hired to investigate and determine whether the Financial Institution's survey site had been compromised and data had been stolen.

### PwC actions



### Computer forensics

The servers hosting the website, including the web server, database server and FTP server, were forensically preserved and analyzed PwC also worked with the client to identify and preserve computers used by web administrators responsible for bank's survey web site.

### Log review

The FTP logs used to transfer files to the web server were preserved. These log files were analyzed to identify unauthorized logins and file transfers to the web server.

### Findings

PwC determined that the work computer of a survey web site System Administrator had been compromised. Further, a brute force attack had been launched against the FTP server. Using the Sys Admin's login credentials, the criminals uploaded malicious web pages to the web site. These false web pages forwarded website visitors to a hostile website maintained by the criminals in an effort to commit Identity Theft. PwC identified all of the incoming IP addresses associated with the unauthorized accesses so the client could cooperate with law enforcement.

PwC determined that PII had not been exposed.

### Remedial actions

#### Respond to data breach allegations

Knowing the facts about the compromised website, the company was in a position to effectively respond to the data breach allegations.

#### Server hardening

PwC helped our client implement best practices for web application development and improved server hardening technologies to help prevent a future computer intrusions.

#### Enhanced security policies

The client implemented enhanced security policies regarding Sys Admin work computers and use of remote access technologies.



# Payment card data breach

## Federal trade commission investigation

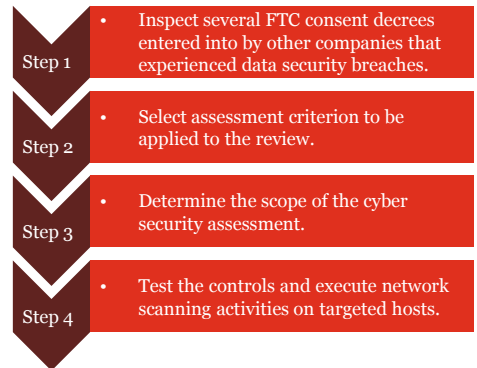
### Client issues

A Global Fortune 500 company experienced a data breach of millions of credit and debit card numbers from their systems, resulting in thousands of known cases of card fraud. As a result of the data breach from 2 years prior, our 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 our client meet compliance obligations.

### PwC actions

After selecting the assessment criterion, PwC implemented a series of workstreams to analyze and benchmark the current state of the company's cyber security. This assessment was performed against a recognized security program framework, International Organization for Standardization/International Electrotechnical Commission 27002:2005. PwC's assessment incorporated the following:

- **Analyze prior reports** - Reviewed security-related documents, including internal reports, audits and third-party assessments.
- **Assessment of security operations** - Interviewed the company's IT management and IT staff to understand the current security operations.
- **Assess controls** - Performed security and control assessments.
- **Data discovery scanning** - Executed limited scanning activities for sensitive PCI and PII data against targeted technology hosts.



### Findings

PwC found that the company's information security program was neither comprehensive nor sustainable, and that it 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 actual operational practices.

### Remedial actions

PwC worked with the client's outside counsel to develop a series of remediation activities bundled into a comprehensive high priority program. This compliance program focused on addressing high priority reactive issues, as well as creating a sustainable program and culture to remediate security issues on an ongoing basis. Listed below are three high priority issues addressed by the program's sustainable and tactical workstreams.

1. **Governance & Culture** – Information security and the protection of customer information should be treated from a cultural perspective in the same way other industry safety regulations are treated at the company.
2. **Technical Vulnerabilities** – The high volume of technical deficiencies results in the organization being vulnerable to sensitive data loss.
3. **People & Process Deficiencies** – The lack of the right people in the correct roles, coupled with confusing and poorly coordinated organizational change, resulted in an exacerbation of the risks associated with information management.



# Stolen laptops containing protected health information

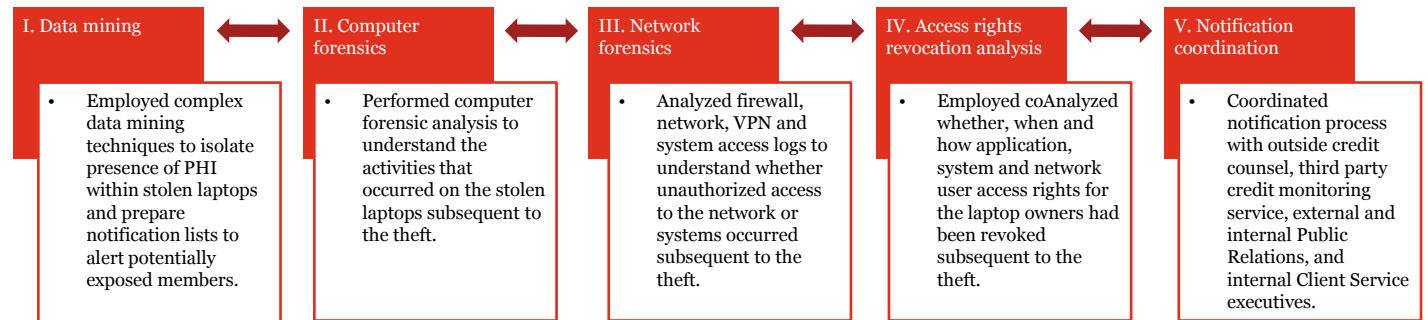
## Compliance with health care data privacy laws

### Client issues

Two “encrypted” laptops containing Protected Health Information (PHI) were stolen from a locked conference room at a client location. These laptops were assigned to IT employees working on a data migration project.

### PwC actions

PwC employed a multi-faceted approach involving data analysis, computer forensic and cyber security professionals to initiate several parallel workstreams to help our client. These workstreams allowed our team to investigate the source of the data breach and begin the process of remedial actions and breach notification coordination in parallel. This approach helped our client illustrate to the government regulators that they were exploring all appropriate methods for investigation and remediation in a timely manner.



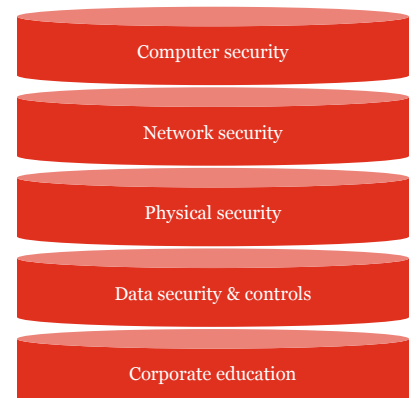
### Findings

A law enforcement investigation determined a security guard responsible for securing the incident location had stolen the two laptops, one of which was recovered by the company. After a thorough forensic analysis of the recovered computer, no evidence was found indicating unauthorized network intrusion or that PHI was accessed after the computer was stolen. Computer forensic analysis determined that IT employees had stored PHI on an unencrypted partition on the local hard drive. The Data Mining exercise determined that over a million members data may have been breached and PwC support the ensuing Breach Notification.

### Remedial actions

PwC worked with the client to implement a series of policy, technical and corporate culture changes, coupled with employee education, to help prevent the risk of future data breaches.

- Computer Security
  - Full Disk Encryption
  - Encryption Training
  - Identity Management/Single Sign On
- Network Security
  - Web Application Testing
  - Network Penetration Testing
- Physical Security and Controls
  - GPS Tracking Devices on Laptops
  - Access Control Changes
- Data Security & Controls
  - PHI Audits
  - HIPPA Risk Assessment
  - Revised Incident Response Procedures
- Corporate Education
  - Stakeholder Workshops with Industry SME
  - Enhanced Employee Training



# Lost backup tapes containing Personally Identifiable Information (PII)

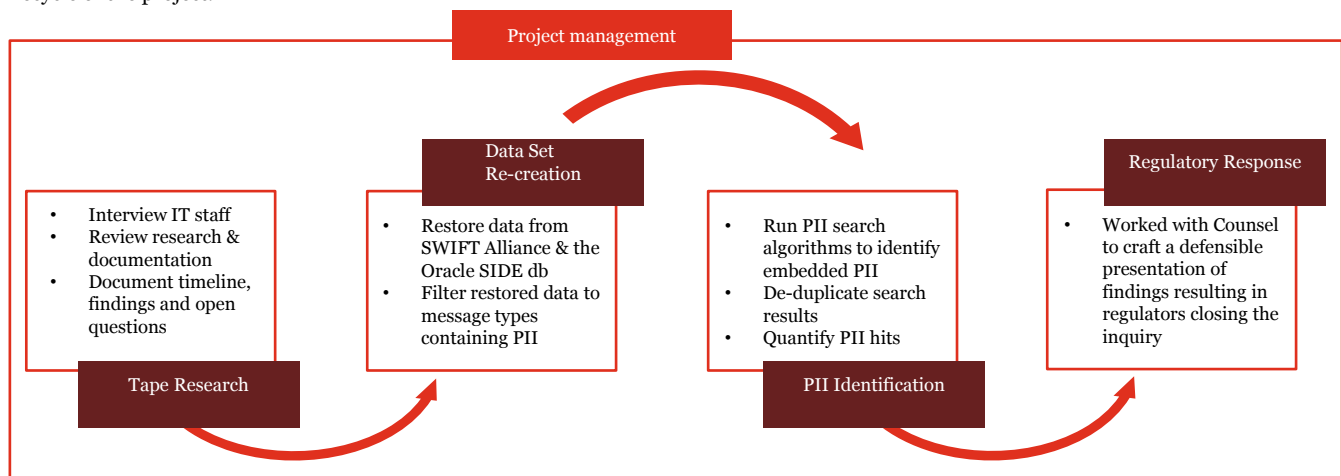
## Financial services regulatory compliance

### Client issues

A Global Fortune 100 company noticed that a series of unencrypted backup tapes were missing. These tapes were used to backup SWIFT transaction data, which provides information about wire transfers between financial institutions. Due to the nature of the transactions, the SWIFT data contains Personally Identifiable Information (PII) regarding the banking customers. After an internal investigation with limited results, PwC was retained to help investigate the lost backup tapes and quantify the exposed PII.

### PwC actions

PwC worked with the company's management and IT department to understand and document the timeline of events related to the missing tapes. In parallel with the tape research and documentation, PwC worked with the database administrators to re-create data population that would have been resident on the missing tapes. After re-creating the dataset, PwC worked with Outside Counsel to develop a defensible approach to identify embedded PII in the SWIFT message data. The following diagram outlines PwC's approach to assist our client, working closely with Outside Counsel throughout the lifecycle of the project.



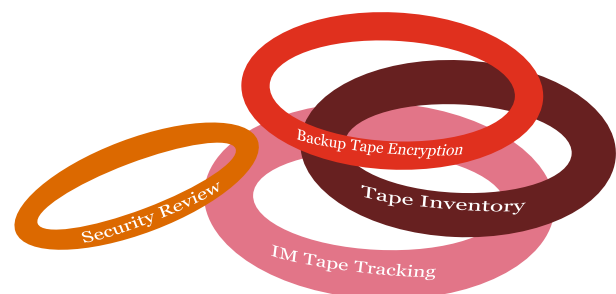
### Findings

After running a multi-tiered PII search including proprietary search algorithms, keyword searches and a manual review on a statistically relevant sample, PwC found PII data in less than 4% of the SWIFT transactions. Working closely with Outside Counsel, PwC documented the technical findings and great lengths an individual would have to go to in order to find embedded PII data. We helped our client and Outside Counsel articulate a case to the Federal Regulator that due to the cryptic format in which this data was stored, an individual being able to extract sensible data is highly unlikely and therefore a disclosure is unreasonable. Ultimately, this decision saved our client millions of dollars in both direct and indirect costs associated with a public Breach Notification.

### Remedial actions/recommendations

Working with Outside Counsel, PwC recommended that the client implement the following remediation programs to help prevent similar issues in the future.

- Backup Tape Tracking
- In-house Tape Inventory Development and Maintenance
- Backup Tape Encryption
- Security Review



# Cybercrime

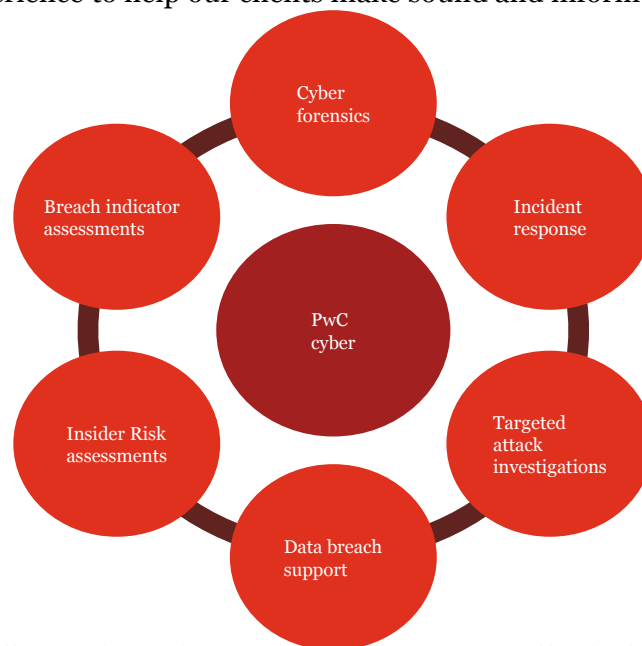
## Forensic investigation & risk assessments

PwC recognizes that organizations today face unprecedented cyber security challenges. Companies must comply with existing and emerging regulations, identify and secure sensitive information that is constantly in motion, investigate breaches and data theft, manage the insider threat, and reduce the gamut of cyber security risks.

**Organizations must be prepared to forensically investigate cyber intrusions, data theft, and insider malfeasance in order to manage legal, regulatory, reputational, and other risks.**

Cybercrimes are committed by a multitude of offenders with various motives: opportunistic global hacker crews, corrupt insiders behaving badly, competitors seeking an advantage, organized criminal enterprises stealing for profit, and foreign governments seeking an economic or military advantage.

PwC works with clients to develop creative approaches to complex cyber-related matters. We combine computer forensics, data analysis, malware analysis, network forensics, cyber security intelligence, fraud investigation and crisis experience to help our clients make sound and informed decisions that will withstand a myriad of inquiries.



PwC helps clients in responding and reacting to cybercrime matters effectively by creating contractual vehicles which permit the quick deployment of our global forensic services resources. As a result, our clients are better positioned to investigate, contain, and remediate cybercrime incidents and manage inquiries from law enforcement, regulators and civil suits.

### Our commitment

We have made a substantial investment to understand the cyber threats that impact your industry and to develop customized solutions that address the needs of our clients. Our global professionals have deep industry and subject matter experience and knowledge. Simply put, they speak your language.

---

## ***For more information, contact***

### **Dave Burg**

Principal

T: (703) 918-1067

E: david.b.burg@us.pwc.com

### **Shane Sims**

Director

T: (703) 918-6219

E: shane.sims@us.pwc.com

### **Kim Peretti**

Director

T: (703) 918-1500

E: kimberly.k.peretti@us.pwc.com

### **Ed Gibson**

Director

T: (703) 918-3550

E: ed.gibson@us.pwc.com

### **David Nardoni**

Director

T: (213) 356-6308

E: david.nardoni@us.pwc.com

### **Tomas Castrejon**

Director

T: (415) 498-8418

E: tomas.m.castrejon@us.pwc.com

---

***[www.pwc.com/us/cyber](http://www.pwc.com/us/cyber)***

***[www.pwc.com/fts](http://www.pwc.com/fts)***

***[www.pwc.com/us/en/forensic-services](http://www.pwc.com/us/en/forensic-services)***

©2010 PricewaterhouseCoopers LLP. All rights reserved.

“PricewaterhouseCoopers” refers to PricewaterhouseCoopers LLP, a Delaware limited liability partnership, or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity.