The Ongoing Challenge of Prevention

From cyber-threats and data breaches to social media scams and mobile attacks, fraud is rampant and rapidly growing. It is an understatement to say that security breaches are a significant issue. Attackers are moving faster, getting smarter, and becoming more agile in their efforts to steal sensitive customer data—with no signs of slowing down. In 2014, more than one billion records were breached worldwide, a 78% increase from the previous year.1

Organizations are constantly challenged with staying one step ahead of fraudsters to protect customer information, company brand image, and revenues. It is unrealistic to think that any organization is immune to attack. One fact is clear: fraud attacks will continue to be a norm in the business landscape, and companies need to be ready.

“In 2014, more than one billion records were breached worldwide, a 78% increase from the previous year.”
—Gemalto and SafeNet

As the worldwide leader in multichannel customer experience management, security is a critical item for Teleperformance. Providing a highly secure environment for our clients, their customers, and our employees is a top priority, so we make sure to offer innovative security solutions that are ahead of the market. The growing, pervasive threat to data security underscores the point that security should be everyone’s responsibility, and ongoing, proactive prevention should be a part of every company’s culture.

This report explores the recent data breach environment from a global perspective and shares information on how Teleperformance is leading the industry with a strong information security system backed by world-class strategies, processes, and technology. Teleperformance continues to raise the bar with its security measures by using a strategy that not only helps to prevent breaches but also anticipates potential threats.

The High Cost of Security Breaches

According to a 2014 global data breach study that included 314 companies from 10 countries, the average total cost of a data breach increased 15% from the previous year, to $3.5 million. A closer look at the results shows that the average business cost loss due to a breach varies greatly between countries (see figure 1), with the highest in the United States at $3.3 million and the lowest in India at $252,876. These costs include abnormal customer churn, increased customer acquisition activities, reputation losses, and weakened goodwill. The differences in cost can be credited to variations in data protection regulations and laws within each country as well as the types of attacks made against companies.

—Ponemon Institute>

Figure 1: Average Business Costs Loss (Ponemon Institute, “2014 Ponemon Cost of Data Breach Study”)
In addition, as figure 2 shows, some of the most regulated industries had significantly higher per capita data breach costs—healthcare ($359), education ($294), pharmaceutical ($227), and financial services ($206)—than the lowest-ranked industries, public ($100) and retail ($105).

Figure 2: Per Capita Cost by Industry Classification (Ponemon Institute, “2014 Ponemon Cost of Data Breach Study”)
A global occupational fraud study carried out by the Association of Certified Fraud Examiners (ACFE), based on 1,483 occupational fraud cases investigated by CFEs, gives evidence of how some breaches are happening as a result of weak internal controls (see figure 3). The study found that “fraud schemes that occurred at victim organizations that had implemented any of several common anti-fraud controls were significantly less costly and were detected much more quickly than frauds at organizations lacking these controls.” Moreover, the widespread and increasing number and cost of security breaches demonstrates an urgent need for proactive detection and prevention measures.

Figure 3: Primary Internal Control Weakness Observed by CFE (Association of Certified Fraud Examiners, “Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study”)

*Other-category was not included in the 2010 Report
Teleperformance’s 5 Pillars of Security and Fraud Prevention

The emphasis of Teleperformance’s security and fraud prevention program is to prevent fraud when possible and detect fraud activity in an early stage, when prevention is not possible. Since the introduction of the fraud risk assessment, the program has matured and includes continual monitoring and auditing to minimize risk and improve compliance with the fraud risk treatment plan. The program is organized according to five main pillars, which form a framework for a comprehensive, proactive approach to fraud prevention:

- **Highly Trained People**
- **Cutting-Edge Technology**
- **Well-Defined Security Processes**
- **Security Management Methodologies**
- **Stringent Policies**
I-Highly Trained People

One of the fundamental aspects of a successful and effective security strategy is recruitment and selection of the right people. Since Teleperformance is a “People Business,” the human resources team plays a key role in managing the company’s most valuable asset—its people. Teleperformance’s HR professionals follow a step-by-step method when hiring new people, which include background checks for all employees specific to past employers, criminal history, and all checks as permitted by local law, such as drug testing. In addition to screening employees for security, the hiring process uses an analytical solution with a predictive model that provides a recruiting score. This score is an indicator for correct job matching, which reduces attrition and recruitment costs locally and globally, improves performance, and allows better hiring decisions. Further, Teleperformance works with each client to create a customized hiring profile specific to client requirements and program needs.

Clear Communication
We have continuous and clear communication on stringent security practices, which promotes a culture of protection and security. From identification badges to screen savers and posters, all have security symbols and language to remind employees of the high standards and awareness for fraud prevention. This type of internal campaign puts security at the forefront of all activities in a contact center, and fosters a strong security culture. The best method to prevent employee fraud, according to the ACFE, is to educate employees (and would-be perpetrators) about the controls in place that will detect fraudulent activity, as well as the likelihood of getting caught and the consequences when caught.

Certified Security Team
A key feature of Teleperformance’s global security team includes security analysts, security consultants, risk consultants, compliance specialists, and auditors that hold a wide variety of certifications, such as:
- CISSP (Certified Information Systems Security Professional)
- CFE (Certified Fraud Examiner)
- CISA (Certified Information Systems Auditor)
- ISO Certified Lead Auditor and Project Management Professional (PMP)

Global Security Playbook
The global security playbook consists of detailed guidelines on security policies and standards. Again, emphasizing the importance of providing clear communication, the guidelines are fully descriptive and illustrated with tools, screenshots, photos, and videos. A virtual tour video offers employees a look at some of Teleperformance’s Best-in-Class sites.

2-Cutting-Edge Technology

Teleperformance invests in cutting-edge tools and technologies to provide an excellent customer experience that is safe, secure, and efficient for clients and their customers. The company’s proprietary technologies and tools help its partners to save on costs associated with updating or replacing outdated IT infrastructures. Numerous industries, such as credit cards, banking, and e-commerce, have stringent regulations and laws for security and consumer protections against fraud and identity theft. Outsourcing partnerships can make companies aware of new developments and security requirements, helping them to avoid costly and unending investments for technology and system upgrades.

Beyond the standard firewalls, anti-viruses, and other commonly used security technologies, Teleperformance utilizes multiple technologies designed to improve the end customer security experience, prevent fraud and maintain integrity and privacy of personal identifiable information, and detect fraud or security risks in real time. For example, there is secured communication technology...
between the customer and agent to avoid verbal exposure of personal identifiable information (PII) such as but not limited to credit card information. This technology securely captures the PII in “non-verbal form” and inserts the PII into the client CRM without ever exposing the PII to the agent.

**TP Security**

Until recently, companies have lacked resources that provide real-time security alerts. Real-time alerts are not only extremely important in rapidly identifying risks but also helping to mitigate costs associated with any data records that may have been breached. Teleperformance’s real-time alert tool, TP Security, provides statistical monitoring technology of agent activities to trigger real-time alerts based upon predefined correlation criteria for each individual client program. Additionally, this technology will shed light on statistical numbers that might represent fraudulent activity and require investigation. Once a security risk is detected, TP Security sends a fraud alert to the security team. This alert includes a detailed agent profile that helps to quickly identify and intercept offending agents.

**TP Policy**

A mapping tool is necessary to manage requirements for compliance, auditing, and reporting. TP Policy maps numerous compliance and legal requirements to client requirements and Teleperformance policies. This tool has reporting dashboard technology that enables a daily view into the exact compliance of the campaign fraud prevention program, and enables midstream corrections so that the program maintains high levels of anti-fraud compliance.

---

### IT Tools and Control

To re-inforce its strong focus on technology and security, Teleperformance has certifications from leading security standards, such as PCI/DSS, ISO 27001/2, and HIPAA. In fact, Teleperformance established the benchmark in contact center information security by becoming the first contact center service provider to achieve PCI/DSS certification. The company has worked closely with technology and security leaders to develop compliance auditing and certification, risk management technology, and secure solutions. As a result, Teleperformance provides a system that detects PCI violations on clients’ systems.

### 3-Well-Defined Security Processes

Teleperformance’s security processes include methods to map data, processes, and operations. This identifies security breaches in processes and systems by utilizing assessments for fraud risk and operations risk.

### Risk Assessment

The fraud risk assessment (FRA), for example, provides a detailed mapping of processes, and system and resource interactions to identify critical points that can create a negative impact or create potential breaches in an operation. To complement the FRA, Teleperformance conducts an operations risk assessment, which involves performing another FRA after 90 days of program management but with a focus on the operational process environment.

After the FRA is conducted, Teleperformance and the client agree on prevention and/or early detection strategies for each discovered risk (“risk remediation strategy”). This involves Teleperformance account management, Teleperformance security analysts, and key individuals from the client to discuss and agree on a treatment strategy for each documented risk. The goal is to agree as a team on the strategy to prevent risks or early detection strategies for risks that cannot be prevented. Following the strategy, the process is implemented as standard practice within the program. While some of the discovered risks may be preventable, some risks require ongoing monitoring for early detection of possible fraud activity. For these ongoing activities, Teleperformance tracks compliance as frequently as needed to ensure the early detection activities are implemented as agreed by both parties. This reporting information will be available to the client on a weekly basis to show actual compliance with each and every risk treatment plan.

### Audit and Certification

To identify any problems within processes and technologies, Teleperformance performs internal and external security audits. Executed by a dedicated team of certified security professionals, the internal audits strive to coordinate and implement security policies throughout the organization. Upon successful implementation of the program and audit, each client and/or operational site is certified to meet the minimum standards within the Teleperformance’s security requirements.
4-Security Management Methodologies

To ensure that its programs are aligned with Best-in-Class security practices, Teleperformance implements the following management methodologies, in addition to many others:

**Security Committee**

As the governing body for Teleperformance’s fraud prevention program, this committee tracks and evaluates global essential security policies and procedures. Additionally, the committee stays abreast of new threats within the market and evaluates these risks to determine if policy changes are necessary.

**Transparent Security Partnership**

A fully transparent partnership between companies is essential for successful, secure multichannel programs. After a program ramp-up, Teleperformance forms security committees with clients in order to share best practices and discuss security breaches identified in assessments.

**Operational Standards Integrated with Security**

All security procedures and policies are integrated with Teleperformance’s operational standards, such as TOPS and BEST. This improves compliance of security policies and procedures within programs and levels within the company.

- **TOPS (Teleperformance Operational Standards)** describes the core operation standards and procedures established to service Teleperformance programs by the operation team. TOPS best practices represent the core framework of the company’s operation management. Its main purpose is to promote usage of the best practices in all contact centers around the world.

- **BEST (Baseline Enterprise Standards for Teleperformance)** includes worldwide best practices for areas such as recruitment and selection, and training and development. BEST benefits include improved practices and metrics at the company, operational, and people level.

5-Stringent Policies

Stringent policies within Teleperformance programs enhance data security for all clients. When team members follow the policies, threats of fraud and data leaks are significantly reduced.

For example, all staff members are well trained on the correct use of social media and the Internet. All workspaces are regulated so employees have only what they need in order to perform their jobs, such as a PC, monitor, headset, mouse and mouse pad, and phone unit—and nothing else. Electronic devices, purses, and bags are not permitted in the program areas.

Workstations have only approved applications and access for web filtering. No removable media devices are allowed. A login/password is required in order to access a program or account. Teleperformance sites have strict facility access controls in place, with assigned identification badges. As an added precaution, Teleperformance provides an employee hotline so employees have a safe and confidential way to report any suspicious fraud activities. The use of hotlines is also highly recommended by the ACFE.

In the fraud cases analyzed by the ACFE in its “2014 Global Fraud Study,” 51% were tips reported for organizations with hotlines, versus 33% reported for organizations without hotlines (see figure 4). This demonstrates a considerable impact that hotlines can have on identifying employee fraud.
Figure 4: Impact of Hotlines (Association of Certified Fraud Examiners, “Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study”)

Tip
Internal Audit
Management Review
Account Reconciliation
By Accident
Surveillance/Monitoring
Document Examination
External Audit
Notified by Law Enforcement
IT Controls
Confession
Other

DETECTION METHOD

PERCENT OF CASES

Organizations Without Hotlines
Organizations With Hotlines

51%
33.3%
15.2%
13.2%
14.6%
17.7%
5.1%
7.9%
4.2%
9.5%
2.9%
1.7%
2%
6.4%
1.3%
5.2%
1.3%
2.7%
1.3%
0.9%
0.6%
0.9%
0.3%
0.7%

Closing Thoughts: Raising the Bar

Although security threats and data breaches are now the norm in the business landscape, there are many ways companies can facilitate fraud prevention and early detection. It starts with having a comprehensive security strategy in place—supported by high-quality policies, processes, and technology—to protect customers and employees. With a strong security culture at the core if its foundation, Teleperformance has helped thousands of companies across dozens of industries provide a secure and extraordinary omnichannel customer experience.

Teleperformance established the benchmark in contact center information security by becoming the first contact center to achieve PCI/DSS certification. Teleperformance’s industry-leading privacy controls have also been recognized with third-party recommendations from MasterCard, and certifications of compliance from ISO 27001/2, HIPAA, and Safe Harbor, among others. Now that certification has become the norm, Teleperformance believes it is time to raise the bar again, and encourages businesses to make a deeper commitment to ongoing information security maintenance work, and promote a security culture within their organizations.
About Teleperformance
Worldwide Leader in Multichannel Customer Experience

We are a People company with a people-centric strategy, interacting with people all over the world. It’s all about People. They are part of who we are and what we do. We analyze their behaviors. We understand their wants and needs. That’s why we deliver outstanding customer experiences through integrated multichannel solutions to enhance customer experience results for our clients.

We are recognized in the market
by leading analyst firms.

“Teleperformance has added innovation to contact center security that often surpasses the client’s internal security controls for fraud prevention and early detection. In short, for companies that absolutely require the highest degree of data and customer information security, Teleperformance is indisputably the industry leader.”

—Michael DeSalles, Industry Analyst, Frost & Sullivan