INFOARMOR®
EMPLOYEE BENEFITS SOLUTIONS

Leveraging Identity and Data Protection as an Employee Benefit to Enhance Enterprise Security

Contents

Executive Summary

In 2014, U.S. businesses were successfully targeted in a series of large-scale cyber attacks that resulted in record-breaking breaches of enterprise, customer, and employee data. So perpetual and stunning were these breaches that some security experts dubbed 2014 “The Year of the Data Breach.” In response to the visibility of these attacks, and their negative impacts on the victim enterprises, many organizations are elevating to the board level all issues pertaining to cyber security (defined as security of business-related technology assets, such as networks, systems, applications, and devices) and data protection (defined as the protection of business, financial, and employee data, as well as enterprise intellectual property). If 2014 was “The Year of the Data Breach,” then 2015 is shaping up to be the year that cyber security and data protection become critical business issues.

Meanwhile, the security community has wrestled with how to address the threat landscape. Emerging technologies and evolving end-user behavior vastly complicate enterprise security, effectively erasing the security distinction between enterprise and employee technologies and data. As a result, traditional security paradigms have proven ineffective in stopping data breaches. Security professionals are now developing adaptive models in response to this new environment. Two important capabilities in newer security models are the early detection and rapid containment of attacks and attackers already inside the enterprise network.

An effective technology in today’s adaptive security models is employee identity and data protection (IDP). IDP solutions offer robust capabilities to help employees quickly detect and recover from breaches, which increasingly contain the sensitive data of both employees and employers. IDP solutions bolster enterprise risk management and enhance security, while providing concrete benefits to both employers and employees following a breach. An increasingly popular way of implementing IDP solutions is through employee benefits packages. By offering IDP as an employee benefit, employers can differentiate themselves among job candidates, thereby helping to recruit and retain top talent by demonstrating the organization’s commitment to employee well being.

This paper aims to:

- Illustrate how recent security breaches are motivating organizations to elevate data protection and cyber security to board-level issues
- Explain how employee IDP adds a critical layer to new, adaptive enterprise security models
- Educate readers on common features and capabilities of IDP solutions
- Provide guidance on how IDP can be implemented in an organization via employee benefits packages and the advantages of this offering to both employees and employers

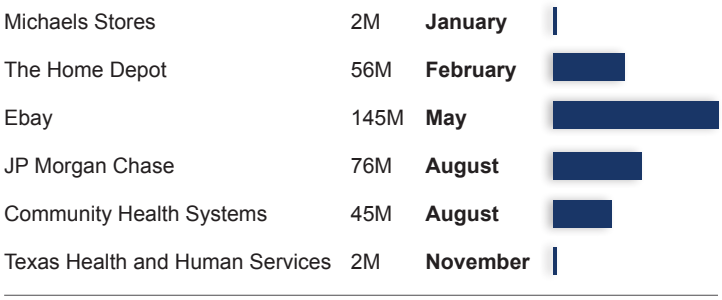
Part I. 2015: The Year Data Protection Becomes a Business Issue

As 2014 began, the business and security communities were still digesting the details and discussing the ramifications of a cyber attack against Target Corporation, which was discovered in December 2013. At that time, the Target data breach was rumored to be larger (in terms of the number of records stolen) than the 2005-2007 breach of TJMaxx, which surpassed 45 million stolen credit card numbers [1]. Target would eventually report that credit card numbers and personal information (phone numbers, mailing addresses, email addresses) were stolen from more than 110 million customers [2], costing the company $158 million to resolve over the course of a year [3]. (Target's breach-related gross expenses as of November 2014, a year following the incident, were $248 million, but insurance covered $90 million of those expenses. This number does not include the damage to its brand [in turn causing customers to shop elsewhere] or the cost of the breach to other organizations, including the estimated $200 million to credit unions and community banks to reissue 21.8 million cards [2].) The Target breach resulted from the hack of a third-party HVAC vendor[4].

As we entered 2015, the business and security communities were once again abuzz about another potentially record-breaking data breach, this time of Sony Pictures Corporation. The Sony breach is estimated to be one of the largest in history, with over 100 terabytes of data stolen[5]. While the Sony breach did not include customer credit card data, it did involve sensitive corporate data and intellectual property, ranging from confidential employee information and corporate emails to the scripts for unreleased movies and the credentials for accessing Sony's information technology networks, systems, and applications [6].

In between the discovery of the attacks on Target and Sony, eBay (145 million records breached), JP Morgan Chase (76 million records breached), Home Depot (56 million records breached), and Community Health Systems (45 million records breached) all suffered large-scale, high-profile data breaches [7]. (Refer to the nearby graphic of recent major data breaches.)

2014 Major Data Breaches: Number of Records Stolen



Source: Privacy Clearinghouse (2014)

Just two months into 2015, the health care and security communities learned of a data breach at Anthem Inc., the second largest health insurer in the U.S. This breach is believed to be one of largest in history to be suffered by an insurance company and includes an estimated 80 million individuals' personal private information (PPI), such as name, street address, email address, employment information, and medical identification/social security numbers [8]. Within days of Anthem discovering suspicious activity on its network, health insurers Premera and LifeWise also identified potential breaches [9]. Those have since been confirmed, with Premera announcing it will notify 11 million customers and LifeWise 250,000 customers of the breaches

that potentially exposed the same types of personal information that was stolen in the Anthem breach [9]. The PPI potentially compromised in these breaches, and the resulting risks to victims, is very different in nature from other recent breaches, such as Target and JP Morgan Chase. These latter breaches primarily involved credit card numbers. Consumers are not liable for fraudulent charges on credit cards. The type of data stolen from Anthem (e.g. social security numbers, medical identifications, etc.) could result in newer types of fraud, such as health care-related scams, which can be more difficult to detect and remediate.

The quantity and severity of these breaches are motivating businesses to elevate the importance of cyber security (defined as security of business-related technology assets, such as networks, systems, applications, and devices) and data protection (defined as the protection of business, financial, and employee data, as well as enterprise intellectual property). For instance, for the first time, cyber security was the major topic of discussion in February 2015 at the World Economic Forum held in Davos, Switzerland, where business and government leaders from around the world gather to discuss trends and issues facing their organizations and countries [10 and 11]. Corporate and university boards are increasingly focusing attention on cyber security and data protection [12], perhaps in part motivated by the firing of Target CEO Gregg Steinhafel following the 2013 breach [13]. How to quantify the risk of cyber attacks and insure against them is currently a major topic of discussion in commercial insurance circles [14]. All of this points to one overarching trend: If 2014 was the year of the data breach, then 2015 is shaping up to be the year that cyber security and data protection become critical business issues.

If 2014 was the year of the data breach, then 2015 is shaping up to be the year that cyber security and data protection become critical business issues.

Businesses are already acting on these increased concerns. For instance, a recent Ponemon Institute study found that 61% of survey respondents saw an average increase of 34% in their security budgets during 2014, mostly in response to high-profile data breaches [15]. Another study forecasted that companies, for the first time, are projected to spend more on data protection than compliance audits in 2015 [16].

One way to enhance enterprise security is by providing employee identity monitoring and data protection (IDP). IDP is a group of technologies designed to monitor credit and non-credit sources of information tied to an individual in order to detect and alert of suspicious and potentially malicious activity targeted against the individual's identity and/or credit. In the event of a successful breach of identity or credit information, IDP offers insurance and other forms of assistance in restoring the victim's identity and credit. Common IDP features and capabilities are explained in more depth in Part 3 of this paper.

An increasingly popular way to offer IDP solutions is through employee benefits packages. Many employers (and employees) still think of benefits as being limited to traditional offerings, such as health insurance and retirement benefits. However, in 2013, 25% of employers offered some form of identity protection [17]. It is forecasted that 20% of employers who do not currently offer identity protection are considering adding it to their employee benefits packages in 2015 [17].

This forecasted growth trend represents an opportunity for brokers and consulting firms who provide employee benefits to expand their traditional offerings to include employee IDP. In doing so, brokers and consultants can differentiate themselves from their competitors and offer a service that is top-of-mind for business leaders in 2015. Organizations are interested in offering IDP as a benefit not only because it protects employees. Security savvy organizations recognize that IDP also adds a critical layer of protection to enterprise security.

Part 2. How Protecting Employees' Identities and Data also Safeguards the Enterprise

The security challenge facing enterprises partially stems from emerging technologies and evolving employee behavior, which enable personal and enterprise technologies and data to overlap in everyday usage. Some of these emerging technologies and sources of data overlap include the following:

- **Cloud Computing** – Cloud computing allows employee on-demand, pay-per-use access to resources such as networks, servers, applications, and services, as well as data storage. Many business end users now leverage both enterprise (e.g., Salesforce) and personal cloud services (e.g., Dropbox) in the course of their everyday work, with enterprise and personal data intermixed across networks, applications, devices, and storage media. For instance, a traveling employee who needs to quickly share a financial spreadsheet with a co-worker may opt to use a personal Google Docs account instead of enterprise resources. Human resources employees commonly use cloud-based software for tasks ranging from recruiting to change management during mergers, acquisitions, and reorganizations. The risk is multifaceted, but can be summarized as follows:
    - If an enterprise cloud server is compromised, it can contain employees' personal data;
    - If an employee's personal cloud service is compromised, it can contain enterprise data.
- **Bring Your Own Device (BYOD)** – BYOD enables end users to incorporate personal devices into their work. Business users appreciate BYOD because it enables them to maintain one, rather than two or more, devices for personal and work use. However, if an employee's device is lost, stolen, or hacked, then enterprise data ranging from email and sensitive files to account credentials can be at risk.
- **Social Media** – Social media enables employees to create and manage accounts and public profiles on social networks. The rise of social media has resulted in an unprecedented amount of publicly available information about enterprises and employees. Employees often share career-related information in personal accounts on social media sites and can reveal useful information about the enterprise in professional profiles on business-related social media sites. Hackers and other scammers can harvest this information with relative ease and then use it in crafting highly targeted attacks against individuals inside organizations. For instance, in recent years, companies in both the defense [18] and energy [19] industries have come under persistent, sophisticated

spear phishing attacks. Spear phishing incorporates (usually via email) highly targeted information about an individual or the organization to trick end users into compromising their devices, usually by clicking on a link to a malicious web site or by opening a booby-trapped document (e.g., Microsoft Office files containing malicious macros [18]).

These new technologies and the ways in which employees use them point to a single overarching trend: Personal and enterprise technologies and data have merged and become indistinct from a security perspective. This trend creates additional risk for the enterprise, stemming from employee decisions about technology and data use. It also creates risk for employees, stemming from employer decisions about enterprise IT and business practices. For instance, based on data reviewed from 2013 enterprise breaches, it was estimated that 15% of personal data breaches originated in the workplace [20].

These new technologies and the ways in which employees use them point to a single overarching trend: Personal and enterprise technologies and data have merged and become indistinct from a security perspective.

Consequently, these emerging technologies and evolving end-user behaviors, which render personal and enterprise technologies and data indistinguishable for security purposes, have shattered the traditional security paradigm of protecting the enterprise network perimeter and the assets within. Now personal and enterprise devices move fluidly into and out of the corporate network on a daily basis, and enterprise data move between enterprise and personal applications, databases, systems, devices, and storage media. Business end users demand these capabilities for convenience and productivity, but the behavior vastly complicates the task of enterprise security.

This has caused the security community to shift its mindset as follows: Prevent as many attacks as possible with layers of traditional security technologies, such as firewalls and antivirus software, but also develop new capabilities for identifying, responding to, and containing what many view as inevitably successful breaches of the enterprise network perimeter. In this model, early detection and rapid containment of attackers and attacks already inside the enterprise network are the keys to minimizing damage. Employee IDP provides one more tool for quickly detecting and recovering from a data breach.

In this model, early detection and rapid containment of attackers and attacks already inside the enterprise network are the keys to minimizing damage. Employee IDP provides one more tool for quickly detecting and recovering from a data breach.

In light of technological trends and evolving security models, employee IDP has become prudent risk management and a valuable tool in the enterprise security suite.

Part 3. Capabilities of Identity and Data Protection Solutions

An employee IDP solution adds an important layer in newer, adaptive security models designed to better protect the enterprise and its employees from new risks and threats enabled by emerging technologies and employee behavior.

Employee IDP solutions vary, but some baseline features usually include the following:

- **Credit Monitoring** – This feature provides continuous credit monitoring, credit scores (updated as frequently as monthly), and credit reports.
- **Insurance** – Insurance protects against out-of-pocket expenses associated with restoring credit, such as lost wages, legal fees, and postage. The coverage amount varies by policy. Victims of identity theft lose an average of between $2,000 and $15,000 in wages resulting from time spent restoring identity/credit during normal business hours, in addition to the expense of required administrative, legal, and related services, which can range from $850 to $1,400 [21].
- **Identity/Credit Restoration** – Identity/credit restoration helps victims of identity theft to recover. This service varies widely, from simple guidance on how to proceed to full-service restoration on behalf of the victim.

Newer technologies and customer demand have spurred innovation. More robust solutions now include one or several of the following features:

- **Digital Wallets** – Digital wallets store a digital copy of important information usually contained in a physical wallet, such as driver's license number, credit card numbers, and insurance cards. If the physical wallet is lost or stolen, then the digital wallet can help to quickly report, cancel, and obtain replacements.
- **Digital Snapshots** – This feature scans the World Wide Web and reports what others can learn about an individual from publicly available information. This report can be used as a guide to minimizing the amount of accessible data that could be used against an employee or the organization in an attack.
- **Reputation Management** – Reputation management monitors and manages social media profiles (e.g., LinkedIn, Facebook, Twitter, Instagram, etc.) to ensure they convey a positive image and do not contain unapproved profile updates or modifications. It can also be an effective tool against cyber bullying and reputation damage on family members' accounts.
- **Controlling Unwanted Solicitations** – This feature reduces telemarketing, pre-approved credit card offers, junk mail, and other unwanted solicitations in order to limit the exposure of personal information.

At the cutting edge is a new category of protection that monitors non-credit sources. This feature monitors high risk transactions, such as online account access, fund transfers, and password resets. (Refer to the nearby graphic for a comprehensive list of non-credit source monitoring and alerts.) The monitoring of non-credit sources is a highly effective security measure, but it is offered in only a limited number of solutions currently available on the market.

The monitoring of non-credit sources is a highly effective security measure, but it is offered in only a limited number of solutions currently available on the market.

Non-Credit Source Monitoring and Alerts

Online authorization	Online transfer	Address change	Phone port change
Account management activity	Online purchase	Fraud inquiry	Payday loan inquiry
Phone insurance claim	Loan application	New account	
Password reset	Medical billing request	Online payday loan inquiry	

Part 4. Advantages to Employers of Offering Employee Identity and Data Protection

Providing IDP for employees provides many advantages. First, and most importantly, in the event of a breach (whether allowed by a lapse in employee or enterprise security or due to malicious intent), IDP benefits both the employer and employee in the following ways:

- *Limit the type(s) and length of exposure* – Risks to and threats against employees now affect enterprise security. Immediate detection of data stolen from an employee – which may include enterprise-related information such as email, virtual private network, or similar account credentials – limits the type(s) and length of enterprise exposure.
- *Maintain employee productivity following a breach* – A single case of identity theft is estimated to take between 58 to 165 work hours to remediate [22]. The total time to restore identity and credit varies widely, with 27.5% taking under six months, 9.6% requiring seven to nine months, and 3.4% requiring from 12 to 23 months [22]. Up to 2.8% of cases take longer than five years [22]. Many IDP solutions include a service to actively help victims of identity theft with resolving issues, which frees employees to remain present and engaged during normal business hours.
- *Decrease employee stress following breach* – Victims of identity theft often report stress, as well as other negative emotions (e.g. anger, depression, etc.), following an incident [21]. This stress can affect concentration, sleep patterns, and other abilities and activities that are critical to remaining healthy. Poor health, in turn, negatively affects work. IDP can decrease the stress associated with identity theft by providing insurance to help pay for expenses and services to help victims restore identity and credit.
- *Peace of mind* – The process of restoring identity and credit is a daunting task, which is fraught with complexity. Many IDP solutions provide an advocate and expert to guide and/or assist victims through the restoration process.

In addition to these benefits, IDP increases the overall attractiveness of employee benefits packages. This improves an employer's ability to recruit and retain top talent, which has been recognized as a strategic and competitive business issue [23]. An employer can differentiate itself among job candidates by offering a robust benefits package:

- Reinforces employees' value to the company
- Demonstrates the employer's interest in the individual well being of its employees
- Illustrates the company is willing to invest in high quality benefits for its employees
- Shows that the company is committed to remaining competitive

Part 5. How to Implement Identity and Data Protection as an Employee Benefit

Employers have flexibility in how to offer IDP as an employee benefit. The two most common methods are as follows:

- *Voluntary enrollment through payroll deduction* – This method enables employees to obtain IDP via the employer benefits package at a discount to retail price. Employees cover the price of the service through payroll deduction.
- *Company-sponsored programs* – With this method, the company covers the total expense of providing the service to its employees. Considering the cost of data breaches to enterprises, which the Ponemon Institute estimated to average $3.5 million per company in 2014 (a 15% increase over 2013) [24], this option can be viewed as a prudent risk management strategy, similar to commercial insurance.

One IDP solution that employers can consider is PrivacyArmor, created by InfoArmor. InfoArmor was the first and is now the largest provider of IDP solutions via employee benefits packages. PrivacyArmor offers the features and capabilities summarized in Table 1 (next page).

Table 1. Summary of PrivacyArmor Identity Monitoring and Data Protection Solution

	Solution	Description
Credit	CreditArmor	Provides continuous credit monitoring, monthly credit scores, and unlimited access to free, online credit score and credit score tracker
Identity	Identity Monitoring	Monitors non-credit sources for high risk transaction alerts in response to suspicious online account access, fund transfers, and password resets, as well as email account monitoring
Digital	WalletArmor	Stores a digital copy of important information contained in a physical wallet, enabling quick replacement of lost or stolen contents
	Internet Surveillance / Digital Identity Report	Scans the "Underground Internet" and provides a report on what others can learn from publicly available information
	SocialArmor	Helps to monitor social media accounts to ensure the maintenance of a positive image and detect cyber bullying and online predators
	IdentityMD	Provides tips, tools, and resources to help prevent identity theft and to restore identity and credit in the event of an incident
Misc.	$25,000 Insurance Policy	Provides for out-of-pocket expenses often associated with restoring identity and credit, such as legal, administrative, and postage fees
	Reduction in Unwanted Solicitations	Limits unwanted telephone solicitations, pre-approved credit card offers, and junk mail in order to limit the exposure of personal information
	Full Service Identity Restoration	Provides full-service identity restoration and identity theft case resolution from start to finish

To learn more about enhancing enterprise security by offering IDP solutions in employee benefits packages, contact InfoArmor via one of the following methods:

- Email: sales@infoarmor.com
- Phone: 1+ 800-789-2720
- Web: Myprivacyarmor.com and infoarmor.com/employee-benefit-solutions/

About InfoArmor

InfoArmor was established to help protect millions of credit cardholders from identity fraud. Today we help businesses fight emerging fraud with industrial strength identity protection, domain, credential, vendor security monitoring, and enterprise threat intelligence services. Approximately 500 groups, including dozens of Fortune 500 companies, rely on InfoArmor to keep their employees, customers, and data secure.

References

1. Vijayan, Jaikumar (March 2007). TJX Data Breach: At 45.6M Card Numbers, it's the biggest ever. [Electronic Resource] Computer World. Retrieved February 13, 2015 from http://www.computerworld.com/article/2544306/security0/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html
2. Krebs, Brian (May 2014). The Target Breach, By the Numbers. [Electronic Resource] Krebs on Security. Retrieved on February 17, 2015 from http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/
3. Target Corporation (November 2014). Target Reports Third Quarter 2014 Earnings. [Electronic Resource] Retrieved on February 17, 2015 from http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1991049
4. Krebs, Brian (February 2014). Target Hackers Broke In Via HVAC Company. [Electronic Resource] Krebs on Security. Retrieved on March 7, 2015 from http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
5. Cook, James (December 2014). Sony Hackers Have Over 100 Terabytes of Documents. [Electronic Resource] Business Insider. Retrieved February 16, 2015 from http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12
6. Greene, Tim (December 2014). Worst security breaches of the year 2014: Sony tops the list. [Electronic Resource] Network World. Retrieved February 13, 2015 from http://www.networkworld.com/article/2861023/security0/worst-security-breaches-of-the-year-2014-sony-tops-the-list.html
7. Privacy Clearinghouse (2014). 2014 Data Breaches. [Electronic Resource] Retrieved February 13, 2015 from http://data-breach.silk.co/s/embed/table/collection/2014-data-breaches/column/records-breached/column/type-of-breach/column/type-of-target/column/city/order/desc/records-breached/suggestion/filter/equals/type-of-target/suggestion/filter/equals/type-of-breach/slice/0/35
8. Swedish, Joseph R. (2015). From the Desk of Joseph R. Swedish, President and CEO of Anthem, Inc. [Electronic Resource] Anthemfacts.com. Retrieved February 9, 2015, from anthemfacts.com
9. ºStaff Report (March 2015). Two More Health Insurers Report Data Breach. [Electronic Resource] Dark Reading. Retrieved on March 24, 2015 from http://www.darkreading.com/two-more-health-insurers-report-data-breach/d/d-id/1319511
10. Kottasota, Ivana (February 2015). Top Executives Freak Out About Hackers. [Electronic Resource] CNNMoney.com. Retrieved February 9, 2015 from http://money.cnn.com/2015/01/22/technology/cyber-crime-risk-davos-world-economic-forum/
11. McFarlin, James (January 2015). Cybersecurity Concerns Seize Center State at Davos. [Electronic Resource] Security Week. Retrieved on February 16, 2015 from http://www.securityweek.com/cybersecurity-concerns-seize-center-stage-davos
12. Help Net Security (February 2015). Security now one of the top risks for business leaders worldwide. [Electronic Resource] Retrieved February 16, 2015 from http://www.net-security.org/secworld.php?id=17930
13. Riley, Michael and Dune Lawrence (May 2014). As Data Breach Woes Continue, Target's CEO Resigns. [Electronic Resource] Bloomberg Business. Retrieved February 16, 2015 from http://www.bloomberg.com/bw/articles/2014-05-05/as-data-breach-woes-continue-targets-ceo-resigns

14. Kenealy, Bill (January 2015). Catastrophe modelers developing cyber risk technologies to assess exposures. [Electronic Resource] Business Insurance. Retrieved on February 16, 2015 from http://www.businessinsurance.com/article/20150104/NEWS07/301049978?tags=%7C299%7C303%7C335

15. Ponemon Institute (January 2015). 2014: A Year of Mega Breaches. [Electronic Resource] Ponemon Institute Blog. Retrieved on March 25, 2015 from http://www.ponemon.org/blog/2014-a-year-of-mega-breaches-1

16 Korolov, Maria (January 2015). Security Priorities Shifting to Preventing Breaches, Improving Internal Controls. [Electronic Resource] CSO. Retrieved February 9, 2015 from http://www.csoonline.com/article/2872310/data-protection/security-priorities-shifting-to-preventing-breaches-improving-internal-controls.html?phint=newt%3Dcso_salted_hash&phint=idg_eid%3D358f6d9e1cf6d0bcc452789380d3722e#tk.CSONLE_nlt_salted_hash_2015-01-21

17. Towers Watson 2013 Voluntary Benefits and Services Survey. [Electronic Resource] Towers Watson. Retrieved February 9, 2015 from http://www.towerswatson.com/en/Insights/IC-Types/Survey-Research-Results/2013/07/voluntary-benefits-and-services-survey

18. Higgins, Kelly Jackson (October 2014). U.S. Military Officials, Defense Firms Targeted in 'Operation Pawn Storm.' [Electronic Resource] Dark Reading. Retrieved February 11, 2015 from http://www.darkreading.com/attacks-breaches/us-military-officials-defense-firms-targeted-in-operation-pawn-storm/d/d-id/1316927

19. Rashid, Fahmida Y. (April 2013). DHS: Spear Phishing Campaign Targeted 11 Energy Sector Firms. [Electronic Resource] Security Week. Retrieved February 11, 2015 from http://www.securityweek.com/dhs-spear-phishing-campaign-targeted-11-energy-sector-firms

20. Risk Based Security (2014). Data Breach Quick View: An Executive's Guide to 2013 Data Breach Trends [Electronic Resource]. Retrieved February 11, 2015 from https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf

21. IdentityTheftFacts.com. (2012). Cost of Identity Theft [Electronic Resource]. Retrieved February 10, 2015 from http://www.identitytheftfacts.com/cost-identity-theft/

22. The Identity Theft Resource Center (2008). Identity Theft: The Aftermath 2008 [Electronic Resource]. Retrieved on February 10, 2015 from http://www.idtheftcenter.org/images/surveys_studies/Aftermath2008.pdf

23. Fernandez-Araoz, Claudio, Boris Groysberg, and Nitin Nohria (2009, May). The Definitive Guide to Recruiting in Good Times and Bad [Electronic version]. Harvard Business Review. Retrieved February 13, 2015, from https://hbr.org/2009/05/the-definitive-guide-to-recruiting-in-good-times-and-bad/ar/1

24. Ponemon Institute (May 2014). Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis. [Electronic Resource] Retrieved February 17, 2015 from http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

INFOARMOR®
EMPLOYEE BENEFITS SOLUTIONS