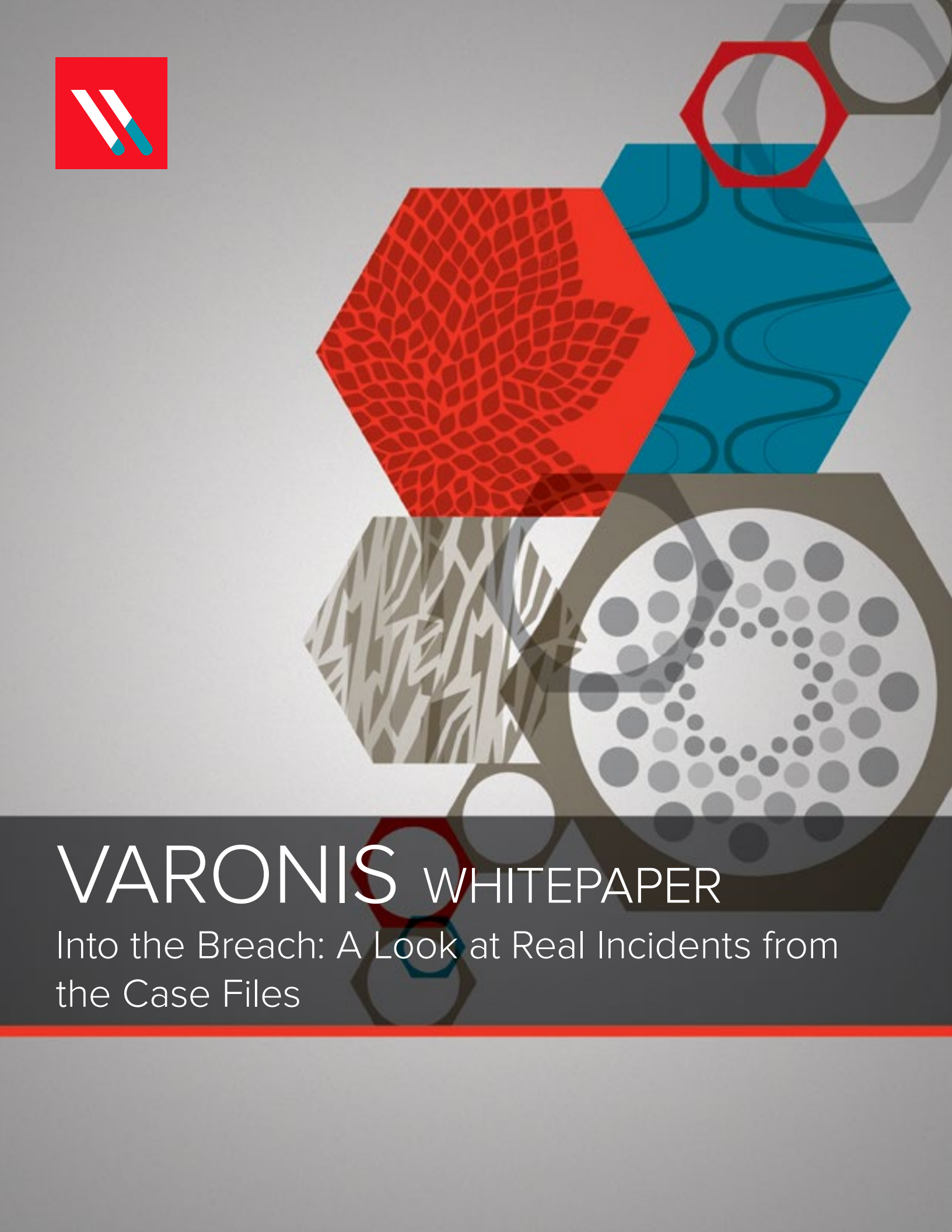


VARONIS WHITEPAPER

Into the Breach: A Look at Real Incidents from the Case Files

CONTENTS

OVERVIEW ____ 3

BREACHES FROM THREE VERTICALS ____ 4

THE MEDICAL INSURER ____ 6

THE MORTGAGE LENDER ____ 7

THE RETAILER ____ 8

LESSONS LEARNED AND CONCLUSIONS ____ 9

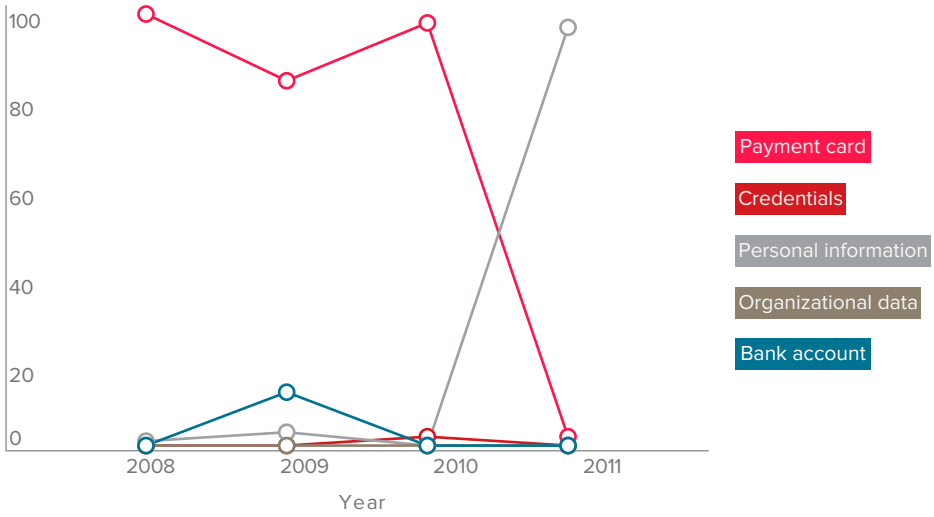
HOW VARONIS CAN HELP ____ 10

OVERVIEW

Verizon's longstanding Data Breach Investigations Report[1], or DBIR, is an excellent starting point to understand the larger trends in security and data protection. The DBIR is based on statistics collected by the US Secret Service, the Dutch National High Tech Crime Unit, and 17 other state and governmental contributors, representing incidents on a global scale. While there may be a few significant one-off breaches, over the years the report has been published—since 2004—key trends have emerged.

For the 2013 report, the DBIR team analyzed over 47,000 incidents from 2012, but were able to validate only about 600 breaches involved in the disclosure of 44 million records[2]. The DBIR statistics should therefore be treated as conservative estimates of breach activity.

TYPE OF BREACHED DATA (% OF RECORDS)



The DBIR tells us that in 2012, companies in financial (37%), retail (15%), and hospitality (10%) led the pack in validated breach incidents, and this group has done so since at least 2008. Not surprisingly, based on these industry categories, the most stolen data is related to transactional information—credit card and other financial data.

In 2011, there was a sudden rise (see chart) of personal data as an object of hackers' efforts. The uptick is mostly the results of attacks against a few major social media sites. This may indicate a new trend. Hackers have been targeting social media to specifically collect personal details along with traditional personally identifiable information or PII—i.e., email, address, and social security numbers. Mining easily attainable personal information instead of encrypted passwords and credit card numbers could lead to more finely tuned faked identities that would be useful in, for example, phishing, pretexting and other "social" attacks.

Over the years, the nature of the threats has mainly coalesced around two types: hacking and malware. For 2012, hacking alone represented 52% and malware accounted for 40% of all breaches. Within hacking, the most common types of threat actions are use of stolen credentials, backdoors, and simple brute-force attacks. Not surprisingly, the DBIR notes that the sophistication level of these hacks is primitive: 78% are classified as requiring low-to-moderate skills.

In the next part of this paper, we'll take a closer look at three representative breaches based on actual incidents in the last few years.

BREACHES FROM THREE VERTICALS

While overall numbers from the DBIR and other breach statistics can give you a good sense of the terrain, it is also quite helpful to review real cases. Why look at specific incidents? For one, executives and others tasked with coming up with their own data protection solutions will gain insight from in-the-trench experiences of others. Second, when you follow a real-world case to its conclusions, many of them have bottom-line consequences: class-action suits, civil fines, and other regulatory penalties. It is instructive for IT staff and other technical executives to see that their security decisions can have a positive financial impact.

We've chosen three cases from the financial and healthcare sectors, which fall under federal as well as state regulations. Primarily, two U.S. federal agencies, the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC), have the power to enforce rules in these areas.

For financial security and privacy violations, the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA), generally come into play. GLBA lays out controls for personal information collected by banks and other financial service companies, requiring them to secure their customers' PII and to restrict who sees this information. The FRCA has a similar structure but is focused on credit report information, which is collected by national credit reporting agencies or CRA, and used by banks and other lenders to determine credit ratings. Both laws are enforced by the FTC.

The Health Insurance Portability and Accessibility Act (HIPAA) effectively defines PII rules for the healthcare sector. HHS has been given the power to write regulations, investigate breach incidents, and enforce the rules through issuing civil and criminal penalties. Its primary leverage is through three broad regulations: the Security Rule, the Privacy Rule, and the Breach Rule. The first describes a series of requirements for protecting health information; the second limits who can see the PII, and the third obligates healthcare organizations to notify their customers (and the HHS) when there's been a breach[3].

More broadly speaking, the previous financial and medical regulations concern themselves with what, for IT security administrators, should be familiar concepts, usually capsulized by the 4 As: Authentication, Authorization, Auditing, and Alerting. For example, HIPAA's Breach Rule covers notification—i.e., Alerting—and its Security and Privacy Rules specify at a high level the technical and administrative safeguards for protecting data, authorizing appropriate access to records, and authenticating persons or entities—Authorization, Auditing and Authentication. A similar viewpoint can be taken towards financial regulations based on GLBA and FRCA. These laws also have their own definitions for who is authorized or "permitted" to access financial data and overall requirements for data security.

In the following cases, which are based on actual incidents investigated by government regulators, it's helpful to read them through the lens of these 4 A's and general IT practices.

THE MEDICAL INSURER

A major health insurance company had implemented extensive web functionality to allow its customer to view and update their insurance information. As part of the process of applying for a new insurance policy, the system returns a URL address to customers. Using the URL, the customer is able to track the progress of the insurance application, as well as review and change existing documents contained as PDFs.

Hackers realized that the URLs had a consistent format and were able to guess the web address of many other customers. They launched an attack that exploited the poor authentication controls on their web site: hackers were able to download thousands of PDF documents containing PIIs—including social security numbers—and other sensitive information without having to validate their identity. Due to inadequate IT auditing controls, the attack went unnoticed until a customer alerted the health insurance company that he was able to view someone else's health information after accidentally modifying a URL.

Even after being notified of this significant glitch, the company took limited actions to update their URL creation software, and delayed a complete investigation until much later.

After complaints from identity theft victims were filed at federal agencies and an initial inquiry started, the full scope of the health security lapses and hacking attack was revealed. This initiated the next phase of the incident. The Department of Health and Human Services' investigators fined the insurer for not notifying the agency –as required by HIPAA—in a timely manner.

Separately, state investigators also fined the insurer for not notifying the relevant state health agencies. Total fines for violating breach notifications at federal and state levels amounted to well over $100,000.

After further investigation by HHS, the insurer was found to have significant shortfalls in their protection of health data. They were found to have not conducted an "accurate and thorough analysis of the risk to the confidentiality of personal health information on an on-going basis" as part of its security management process required by HIPAA's Security Rule[4]. And more specifically, they did not "evaluate the likelihood and impact of potential risks to the confidentiality" of personal medical information based on breach of their web site. For example, they could have put in place software to detect unusual spikes in access to PDF files that deviate from typical day-to-day usage.

The insurer was ultimately fined $50,000 for violating several aspects of the Security Rule and has submitted to ongoing audits from HHS.

Finally, after alerting over 30,000 of its customers that their personal information was likely stolen by hackers, the insurer paid for credit report monitoring services for a period of 60 days at cost of $50,000.

INCIDENT PROFILE

DATA EXPOSED

- social security numbers
- sensitive patient medical information

IT DEFICIENCIES

- weak authentication
- poor file auditing controls

OUTCOME

fines ($50k)

credit monitoring ($50k)

mandatory HHS auditing

negative publicity impacting customer trust and business results

THE MORTGAGE LENDER

As part of its business operations, a mortgage lending company routinely collects personal data related to its current customers and potential clients. This sensitive data includes credit histories, bank account numbers, social security numbers, and other personal identifiers.

In its credit checking process, the mortgage lender obtains online credit histories from a credit reporting agency or CRA. To log into the CRA's portal, mortgage lender employees need to enter a name, address, and social security number into an online form. The credit reports are stored in the mortgage lenders work area on the CRA portal. However, those reports were also downloaded into the lender's file system.

Over a period of time, hundreds of full credit reports along with name, address, and social security numbers used to access these reports accumulated in a single folder on the file system. Unfortunately, the folder gave permissions to all employees at the mortgage lender rather than restricting access to authorized employees. The folder also contained a file with login information to the CRA portal. In the course of doing business with a real-estate developer, the lender also gave the developer access to its VPN.

After consumer complaints of identity theft, an FTC investigation ultimately revealed that a hacker had gained access to the real-estate developer's network, and then from there was able to enter the lender's network. In addition to transferring existing files containing customer credit histories and social security numbers of over 200 customers, the hackers also obtained the login information to access the CRA portal. By generating random social security numbers, the hacker was able to download and transfer an additional 50 reports.

The FTC had found that the lender had not made a reasonable security assessment of the risks in its file system and in its network access polices for third-parties, had not taken reasonable steps to address these risks, and had not specifically reviewed the full scope of protected data in its folders.

Eventually the FTC also found the lender had violated several parts of the Safeguard Rule of GLBA, including lack of security assessment, not designating an employee to coordinate a corporate security program, not implementing security safeguards for the file system with respect to PII and continually monitoring its file controls, and finally not insuring that third parties had similar protection for PII that it held. In addition, since credit information had been compromised, the lender had been found to violate the FRCA by effectively furnishing reports to hackers who did not have "permissible" reasons to look at the report.

While the FTC did not issue any fines, the lender was required (under GLBA) to implement "a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information."[5] It was also required to undergo continual audits of its security program for a period of 5 years.

INCIDENT PROFILE

DATA EXPOSED

- credit reports

IT DEFICIENCIES

- poor file auditing controls
- broad authorizations for sensitive data

OUTCOME

- five years of mandatory FTC auditing

THE RETAILER

A nationwide retailer had introduced a wireless point-of-sale system in its stores. It connected existing check-out registers to the network as well as allowing mobile payment-acceptance devices to be used by the sales staff. Their WiFi network unfortunately had minimal security and encryption configurations—devices were set to use Wired Equivalent Privacy or WEP, an outdated and highly vulnerable wireless security protocol. At some point, hackers—believed to be from an eastern European cybergang—were stationed outside a store. They captured packets over the WiFi network and eventually were able to learn or guess employee passwords to access the company's main network at their headquarters.

The company had been certified under Payment Card Industry or PCI security standards, which requires encryption of credit card information.[6] Unfortunately, broadly permissioned clear-text files containing credit card numbers, bank routing and account numbers, name and address information, and social security numbers of customers were found on the retailer's file servers by the hackers. Weak or non-existent user validation controls—e.g., lack of two-factor authentication—allowed the hackers to gain remote access to these critical assets and eventually to directly download the files. It is believed at some point they placed malware on the servers to automatically push files to the criminals' own computers. Poor IT auditing of file transfers allowed hackers to continue their activities for at least a year without their being detected.

Identity theft complaints filed with regulators allowed federal investigators to eventually trace the breach to the retailer. After further analysis, the retailer realized that several million credit card numbers had been compromised over a period of at least two years. Once the enormity of the breach was realized, the CEO publicly announced the incident, and the retailer directly informed banks, credit card processors, credit reporting agencies, as well as Visa and Mastercard with more details.

The eventual cost to the retailer for the breach was well over $100 million. The retailer had to settle class action suits from consumers and banks for negligence, and pay claims to the credit card companies for issuing millions of new cards. The retailer also agreed to an out-of-court settlement with several state attorneys general to improve the security of their system. Finally, since aspects of FRCA had been violated, the company had to pay fines to the FTC, as well as submit to continual audits.

INCIDENT PROFILE

DATA EXPOSED

- social security
- credit card
- bank routing numbers

IT DEFICIENCIES

- vulnerable WiFi security
- weak authentication for remote users
- poor IT auditing controls

OUTCOME

- class action
- other lawssuits ($100 million)

LESSONS LEARNED AND CONCLUSIONS

From the perspective of IT security, one key lesson is that the actual exploits and attack mechanisms were fairly simple. The methods of the retailer's attackers—again this is based on an actual incident—involved nothing more complicated than eavesdropping on a poorly secured wireless network. This particular corporate victim, obviously, could have done more to protect both its store networks and more importantly its internal corporate network. In general, though, as is emphasized in the DBIR, hackers have been successful at walking through the front door of many of these networks.

This leads to the next point. Once inside, the hackers went about looking for files containing PIIs. In these incidents, and in most cases where there has been a major breach, sensitive information is all too readily available. Credit card numbers, financial information, and health insurance IDs are often found in poorly permissioned folders and files. To make matters worse, the data is typically unencrypted.

There's nothing necessarily "wrong" with having this unstructured clear-text data available if authorized employees need this information to do their jobs. But without other preventive and detective controls (regularly reviewed access control lists, auditing and alerting), this critical information is clearly inadequately protected. In fact, one of the key IT lapses that contribute to a breach's seriousness is the limited attention paid to restricting folder permissions to only those employees truly authorized–because of a job function or role--to access the data.

The third point related to these breaches is that the hackers went about their work over a period of months, and in one case above, at least a year, before being spotted. The actual detection of the breaches occurred indirectly—through the complaints of identity theft victims— and was too late to affect any outcomes. While many companies deploy anti-viral or anti-malware software, port monitoring software, and other hacking detection mechanisms, they do little good when the hackers have gotten inside the network using legitimate logins—guessing default admin passwords or exploiting poorly conceived user passwords.

This is where a "Plan B" becomes important. Since some attacks will inevitably get through, a mitigation strategy then becomes critical. Over the years, the DBIR has included many recommendations is this area, but two bullet points that always seem to show up in their lists are "audit user accounts" and "monitor and mine event logs".

One important overall approach to limiting the liabilities of a breach comes from a relatively new concept known as "privacy by design."[7] The ideas involved are less about nitty-gritty security measures. They are instead more focused on ensuring that consumers participate in privacy decisions, and requiring companies to build privacy directly into their products and services at the beginning stages. Another important principle in privacy by design is to limit personal data collected from customers to only what is needed for a business function. By minimizing extraneous data, companies can reduce breach liabilities based on the type of social attacks that we mentioned at the beginning of this paper.

Here are a few key principles from privacy by design that would reduce the liabilities of many breaches, in addition to the ones we discussed:

- Give consumers access to their data and allow them to review and correct it. Often data thieves will change addresses and other details, and this can be a clue to the consumer that a theft is in progress.
- Limit the amount of data that is initially collected to what is actually needed for business purposes. More personal data and especially unnecessary PII that's stored as part of an application process increases the risk of exposure and ultimately the cost of a breach.
- Introduce reasonable retention limits into data management—don't store information longer than necessary.

HOW VARONIS CAN HELP

DISCOVER AND PROTECT WHAT'S SENSITIVE

The Varonis IDU Classification Framework is the only solution that identifies the highest concentrations of sensitive data that are most at risk and provides a clear methodology to safely remediate that risk without manual effort.

A built-in report shows you a prioritized list of folders that contain the most sensitive data and the most exposed—through global access groups (Everyone, Authenticated Users, etc.) and/or normal groups that contain too many members. Other metrics can be used to prioritize remediation, including activity, size of files, and density of files.

ENSURE ONLY THE RIGHT PEOPLE HAVE ACCESS TO DATA

DatAdvantage gives you a consistent view of permissions across Windows, NAS, UNIX/Linux, Exchange, and SharePoint. With Varonis you can

- Find and remediate data is that sensitive and overexposed
- Model permissions changes in a sandbox before executing
- Provide data owners intelligent recommendations on where to reduce access to their data
- Clean up unused users and groups
- And much more!

BIG DATA SECURITY ANALYTICS

Varonis logs every user's activity across your entire environment, and uses bi-directional cluster analysis and machine learning to predict which permissions they really need. This helps you eliminate risk and remain compliant.

MONITOR USE, ALERT ON ABUSE

More than 95% of file access activity is not monitored by IT because native auditing is slow and hard to use. With Varonis' sortable and searchable audit trail, you always know who is touching important business data. What's more, you can setup alerts whenever abnormal access activity or privilege escalations happen.

GET RESPONSIBILITY FOR DATA OUT OF IT – SUSTAINABLE SECURITY

DatAdvantage can see who is actually accessing data, so it can lead IT right to the appropriate business owner and get them timely information about their data. DataPrivilege makes it painless for business users to review and authorize access. The end result is the right people, with the right information, making the right decisions.

[1] *2013 Data Breach Investigations Report*

[2] *The DBIR team validates breach incidents by confirming that there had been actual data exposure –records downloaded--and there were enough details recorded to meet its methodology standards. For 2012, there were over 47,000 incidents analyzed, but only 621 were confirmed breaches.*

[3] *Understanding HIPAA Privacy*

[4] *Summary of HIPAA Security Rule*

[5] *GLBA Safeguards Rule*

[6] *Payment Card Industry Security Standards Council*

[7] *Protecting Consumer Privacy in an Era of Rapid Change*

ABOUT VARONIS

Varonis is the leading provider of software solutions for unstructured, human-generated enterprise data. Varonis provides an innovative software platform that allows enterprises to map, analyze, manage and migrate their unstructured data. Varonis specializes in human-generated data, a type of unstructured data that includes an enterprise's spreadsheets, word processing documents, presentations, audio files, video files, emails, text messages and any other data created by employees. This data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property and numerous other forms of vital information. IT and business personnel deploy Varonis software for a variety of use cases, including data governance, data security, archiving, file synchronization, enhanced mobile data accessibility and information collaboration.

Free 30-day assessment:

WITHIN HOURS OF INSTALLATION

You can instantly conduct a permissions audit: File and folder access permissions and how those map to specific users and groups. You can even generate reports.

WITHIN A DAY OF INSTALLATION

Varonis DatAdvantage will begin to show you which users are accessing the data, and how.

WITHIN 3 WEEKS OF INSTALLATION

Varonis DatAdvantage will actually make highly reliable recommendations about how to limit access to files and folders to just those users who need it for their jobs.

WORLDWIDE HEADQUARTERS

1250 Broadway, 31st Floor, New York, NY 10001 **T** 877 292 8767 **E** sales@varonis.com **W** www.varonis.com

UNITED KINGDOM AND IRELAND

Varonis UK Ltd., Warnford Court, 29 Throgmorton Street, London, UK EC2N 2AT **T** +44 0207 947 4160 **E** sales-uk@varonis.com **W** www.varonis.com

WESTERN EUROPE

Varonis France SAS 4, rue Villaret de Joyeuse, 75017 Paris, France **T** +33 184 88 56 00 **E** sales-france@varonis.com **W** sites.varonis.com/fr

GERMANY, AUSTRIA AND SWITZERLAND

Varonis Deutschland GmbH, Welserstrasse 88, 90489 Nürnberg **T** +49 (0) 911 8937 1111 **E** sales-germany@varonis.com **W** sites.varonis.com/de