Data Breaches and ID Theft

What CFOs and HR Professionals Need to Know

THE PARTNERS GROUP

www.tpgrp.com

Introductions

Sarah Friend
Executive Vice President
Sales & Marketing
The Partners Group

Rick Kam
President/Founder
ID Experts

Craig Pankow
Managing Director
Commercial Insurance
The Partners Group

THE PARTNERS GROUP

Agenda

Part One:

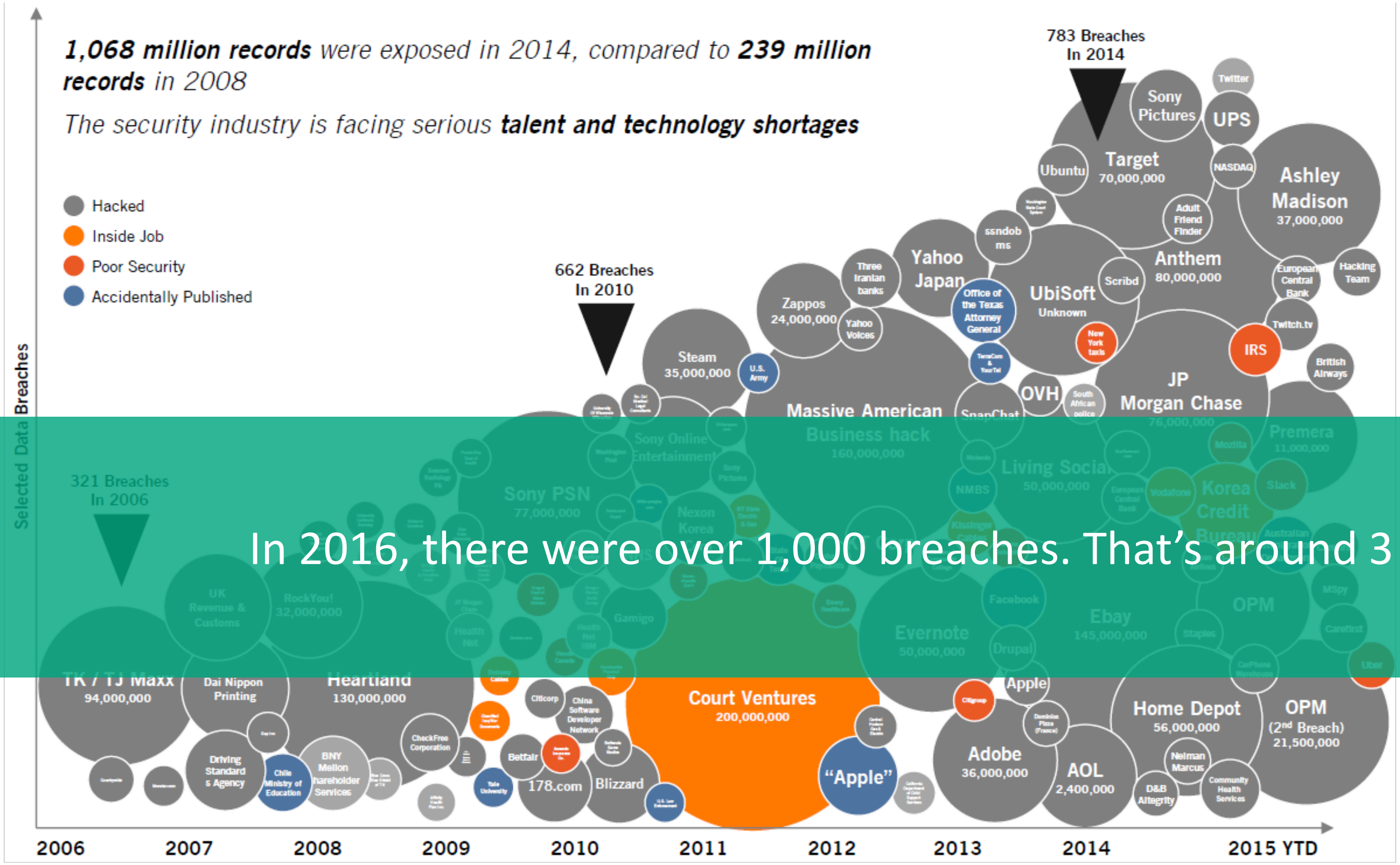
- The risk and impact of data breaches and identity theft to individuals and families
- New threat of medical ID theft and risk to self-funded health plans
- Protecting yourself and protecting your employees

Part Two:

- The risk and impact of data breaches to businesses
- Understanding insurance coverage to protect your business

Data Breach and Identity Theft Risk

Explosive growth in data breaches



1,068 million records *were exposed in 2014, compared to* ***239 million records*** *in 2008*

The security industry is facing serious ***talent and technology shortages***

In 2016, there were over 1,000 breaches. That's around 3 per day.

THE PARTNERS GROUP

Equifax Breach Affects 145.5M

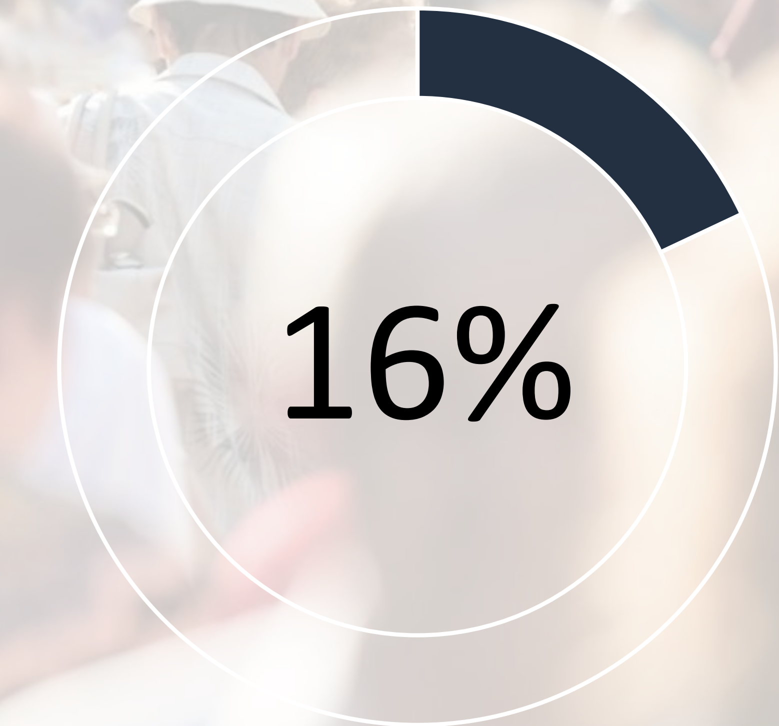
One out of every two employees is potentially affected

THE PARTNERS GROUP

ID Theft a Persistent Problem

15.4MM U.S. consumers victimized by some type of identity theft in 2016. This was up 16% vs the prior year.

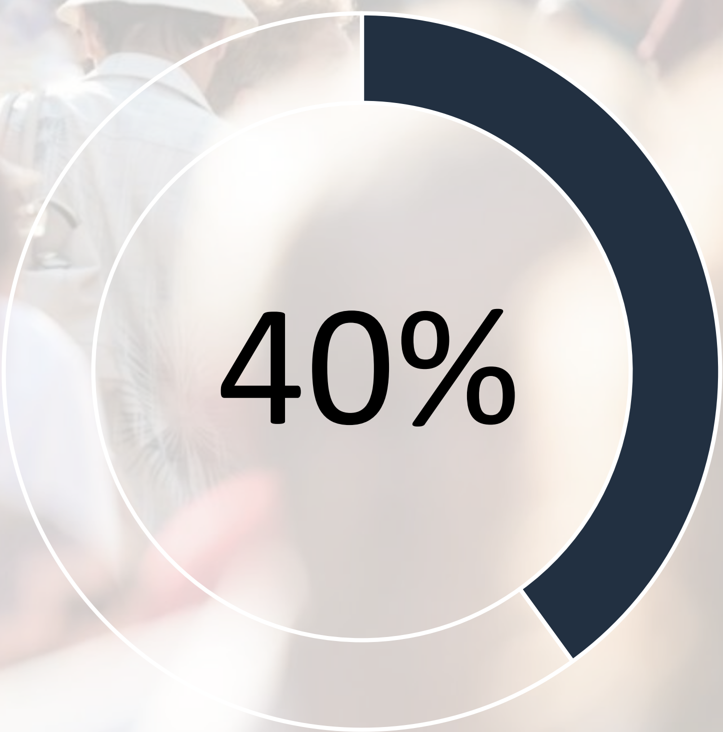
2016 Javelin Research Identity Fraud Study



ID Theft a Persistent Problem

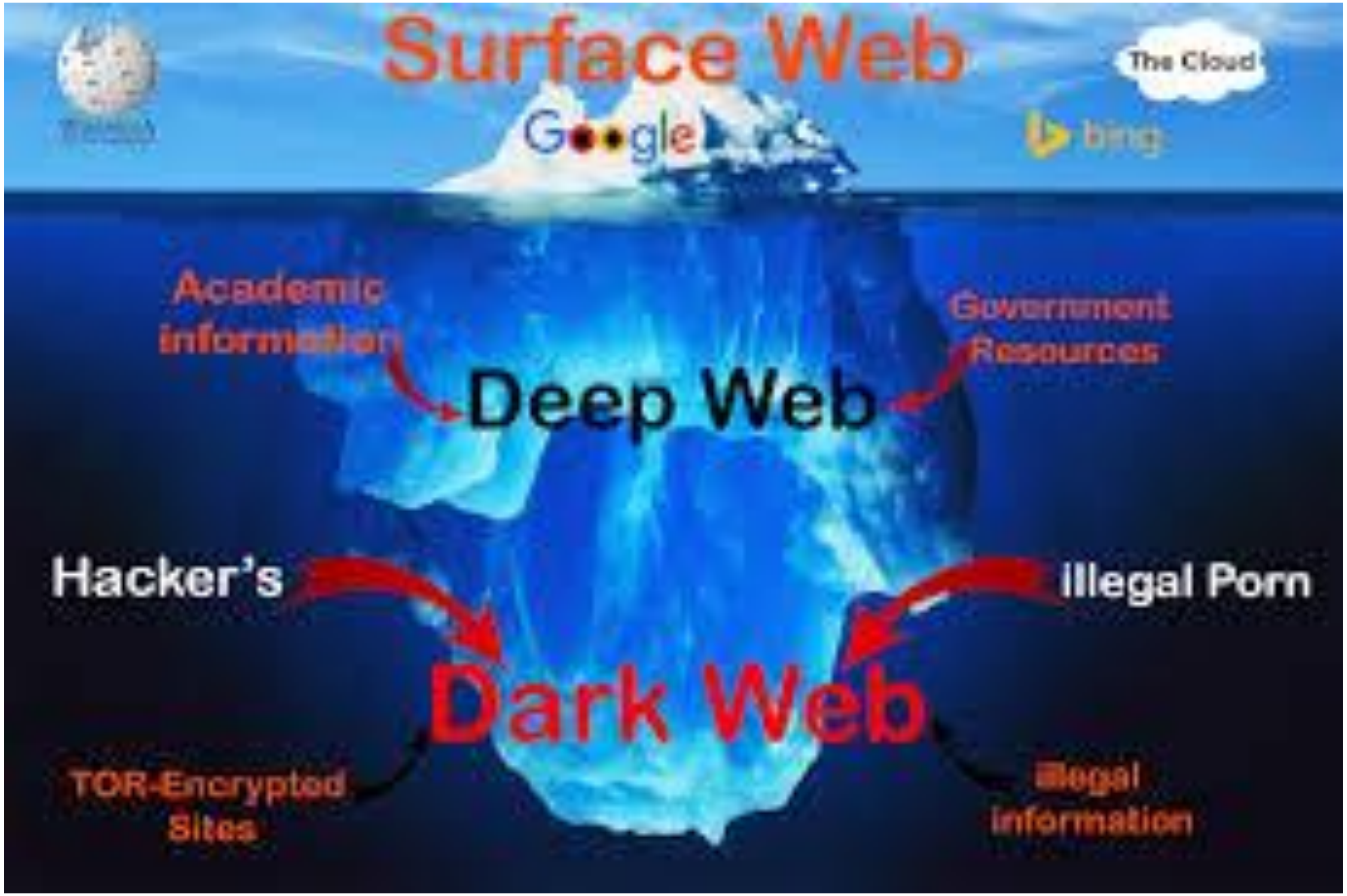
US data breaches tracked in 2016 at an all time high of 1,093, a 40% increase in number of breaches from the prior year.

ITRC Data Breach Report 2016



THE PARTNERS GROUP

Levels of the Internet

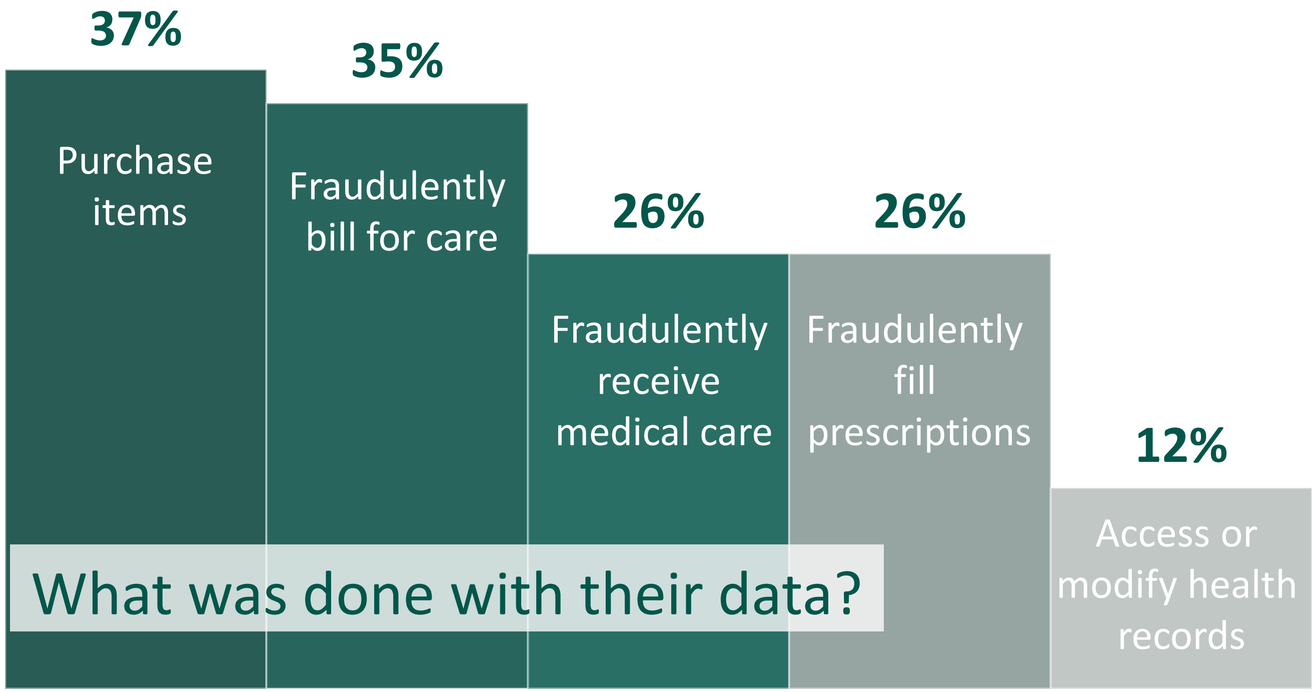


THE PARTNERS GROUP

Health Data is the Next Frontier

Why?

Medical identity is worth 10-20 times more than a credit card or social security number.


What was done with their data?

** Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust*

THE PARTNERS GROUP

Real Story

"To this day, I don't know if my name is in the baby's medical record. It's insidious."

Utah's child protective services called Anndorie Cromar to report that her newborn daughter had tested positive for methamphetamine. But Ms. Cromar hadn't given birth. Someone had stolen her health insurance information, gone into labor, and delivered a baby girl.

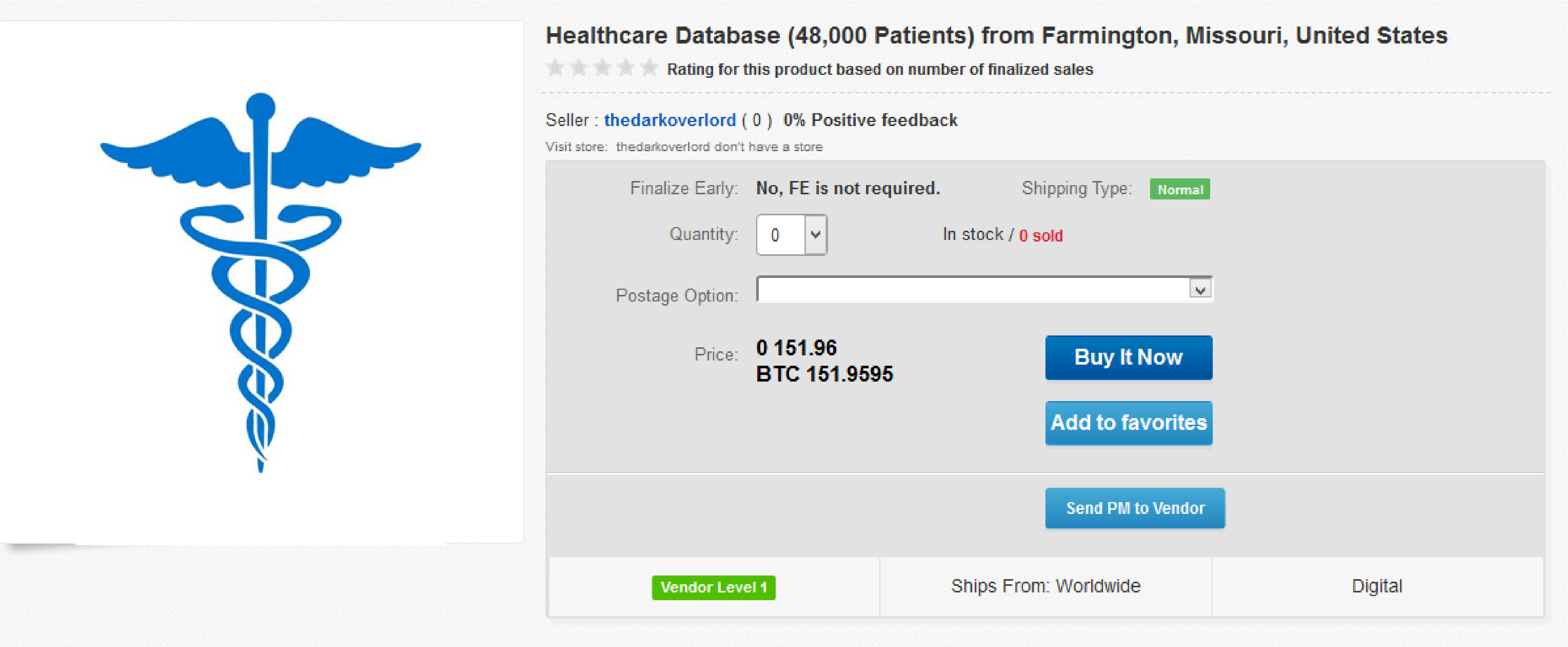
The ordeal took years to straighten out. She was never able to fully settle the hospital bill. She couldn't view her own medical records because they now contained the thief's health information, protected by HIPAA.

She had to go to court to get her name taken off the baby's birth certificate.

See Anndorie's Story:
https://www.youtube.com/watch?v=MQjocgRfuNE

THE PARTNERS GROUP

Healthcare Data Sold on Dark Web



Healthcare Database (48,000 Patients) from Farmington, Missouri, United States

☆☆☆☆☆ Rating for this product based on number of finalized sales

Seller : thedarkoverlord (0) 0% Positive feedback

Visit store: thedarkoverlord don't have a store

Finalize Early:	No, FE is not required.	Shipping Type:	Normal
Quantity:	0	In stock / 0 sold	
Postage Option:			
Price:	0 151.96 BTC 151.9595		

Vendor Level 1 | Ships From: Worldwide | Digital

Reducing Risk of Identity Theft

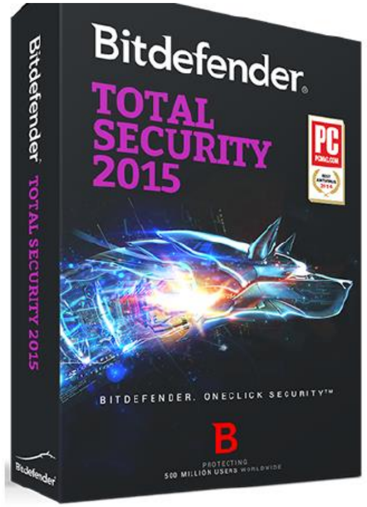
THE PARTNERS GROUP

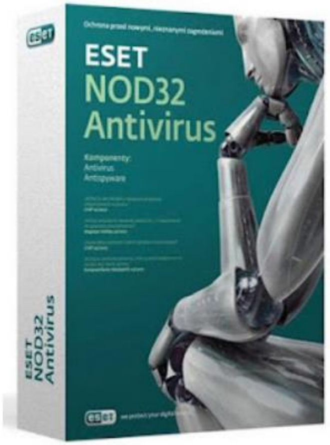
9 Types of ID Theft

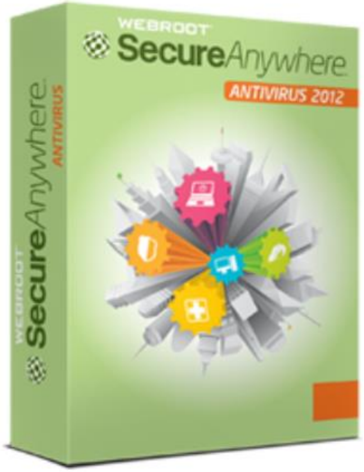
1. Financial
2. Child
3. SSN
4. DMV
5. Criminal
6. Employment
7. Insurance
8. Synthetic
9. Medical

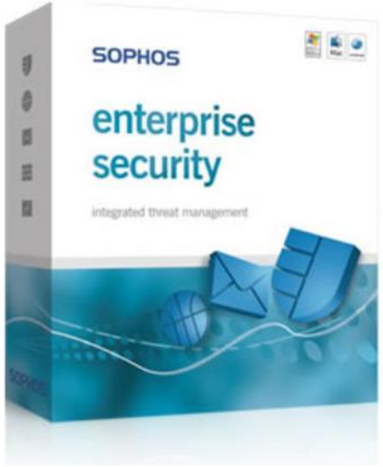
THE PARTNERS GROUP

Anti-Virus Software


Bitdefender
TOTAL SECURITY 2015
BITDEFENDER. ONECLICK SECURITY™
PROTECTING 500 MILLION USERS WORLDWIDE

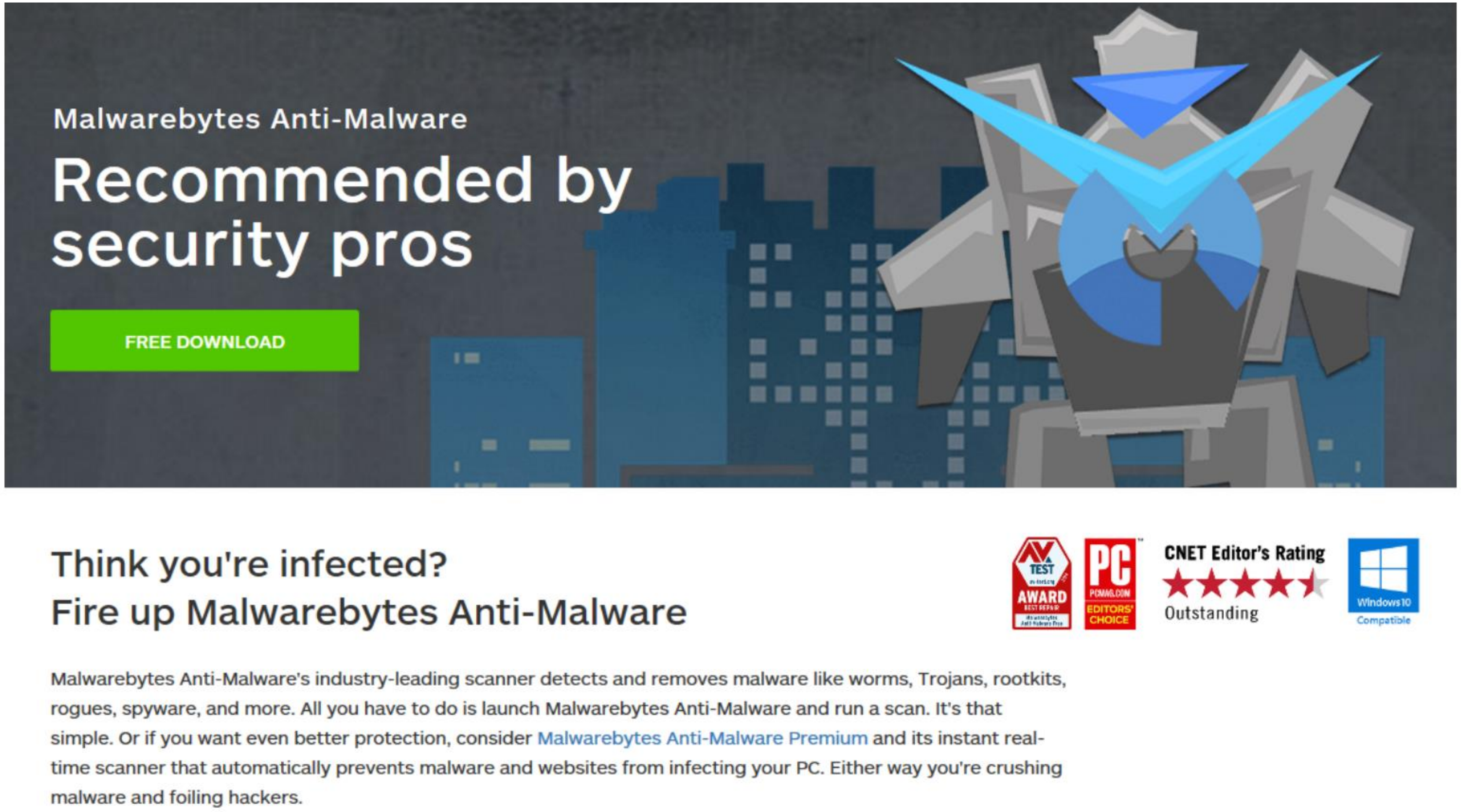






For MACs:

Anti-Malware



Malwarebytes Anti-Malware

Recommended by security pros

FREE DOWNLOAD

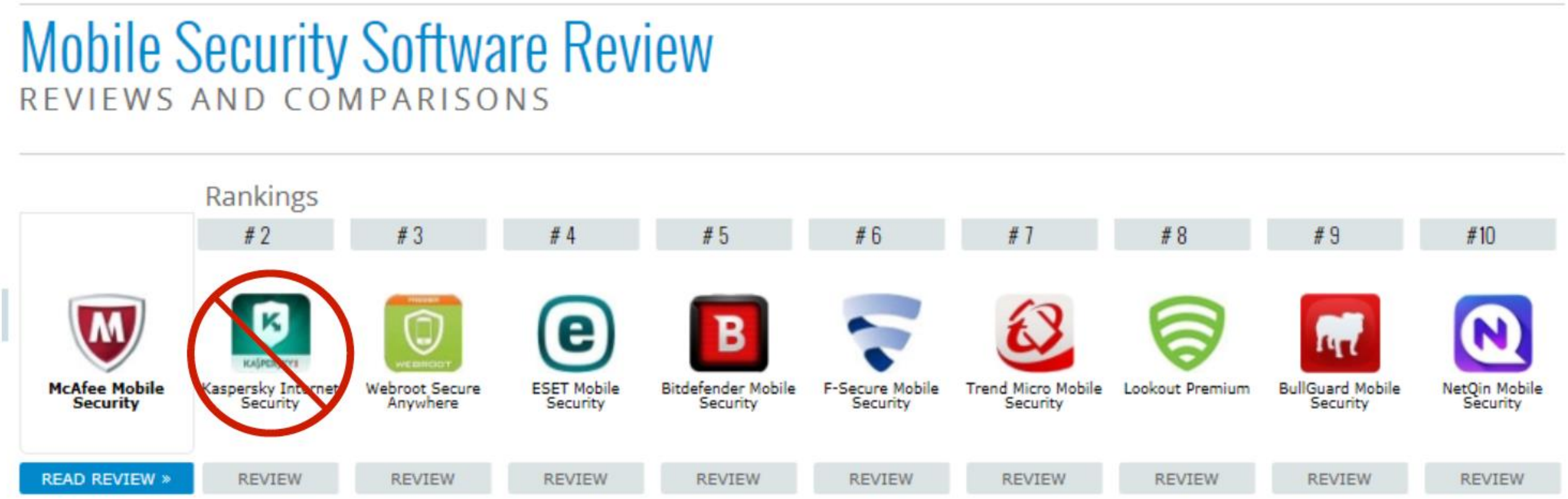
Think you're infected?
Fire up Malwarebytes Anti-Malware

Malwarebytes Anti-Malware's industry-leading scanner detects and removes malware like worms, Trojans, rootkits, rogues, spyware, and more. All you have to do is launch Malwarebytes Anti-Malware and run a scan. It's that simple. Or if you want even better protection, consider Malwarebytes Anti-Malware Premium and its instant real-time scanner that automatically prevents malware and websites from infecting your PC. Either way you're crushing malware and foiling hackers.

https://www.malwarebytes.org/antimalware/

Anti-Virus for Smartphones

- YES, they are available
  - http://mobile-security-software-review.toptenreviews.com/



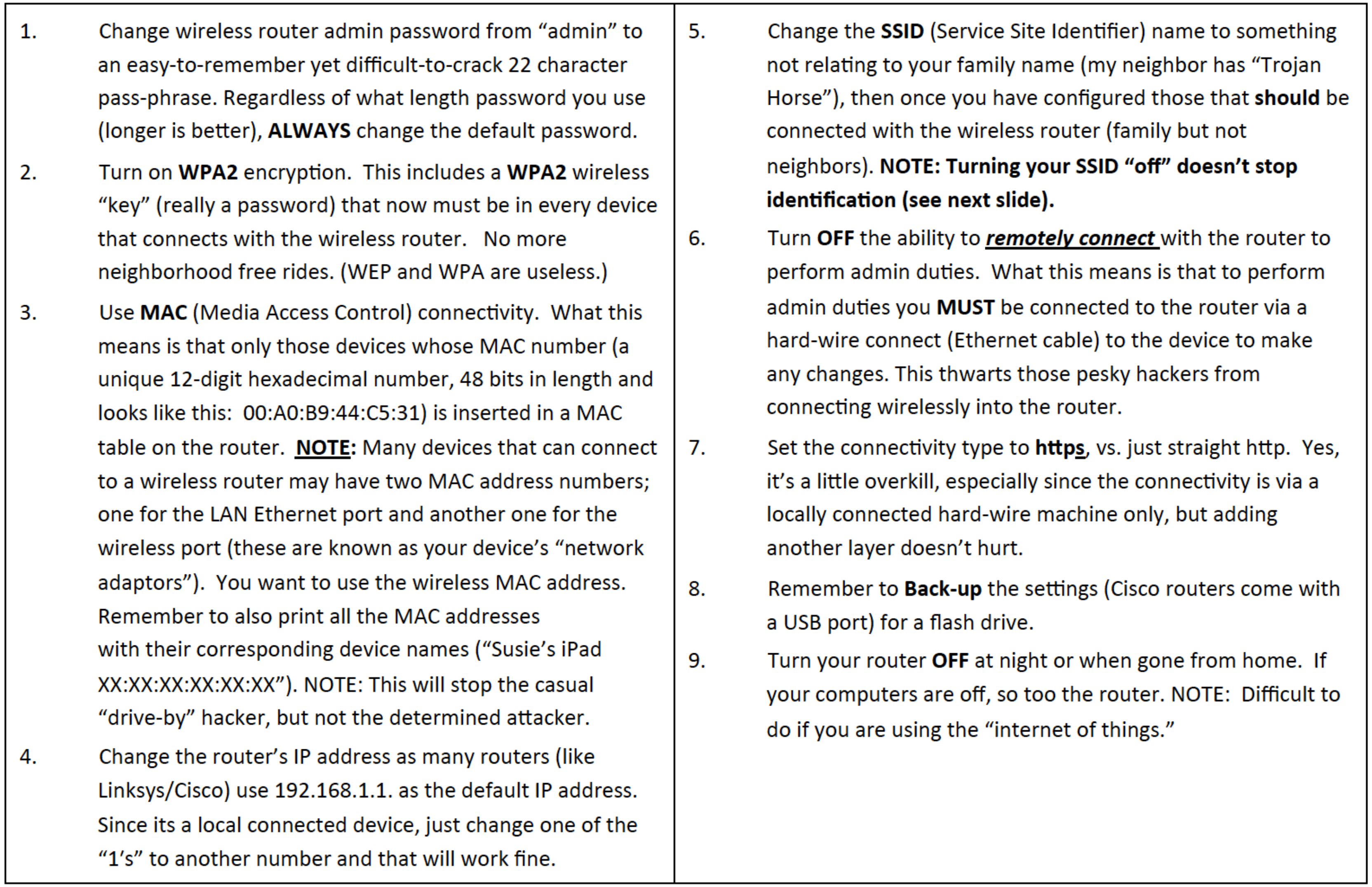
Mobile Security Software Review

REVIEWS AND COMPARISONS

Rankings

	# 2	# 3	# 4	# 5	# 6	# 7	# 8	# 9	#10
McAfee Mobile Security	Kaspersky Internet Security	Webroot Secure Anywhere	ESET Mobile Security	Bitdefender Mobile Security	F-Secure Mobile Security	Trend Micro Mobile Security	Lookout Premium	BullGuard Mobile Security	NetQin Mobile Security
READ REVIEW »	REVIEW	REVIEW	REVIEW	REVIEW	REVIEW	REVIEW	REVIEW	REVIEW	REVIEW

Secure Your Wireless Router



1. Change wireless router admin password from “admin” to an easy-to-remember yet difficult-to-crack 22 character pass-phrase. Regardless of what length password you use (longer is better), **ALWAYS** change the default password.

2. Turn on **WPA2** encryption. This includes a **WPA2** wireless “key” (really a password) that now must be in every device that connects with the wireless router. No more neighborhood free rides. (WEP and WPA are useless.)

3. Use **MAC** (Media Access Control) connectivity. What this means is that only those devices whose MAC number (a unique 12-digit hexadecimal number, 48 bits in length and looks like this: 00:A0:B9:44:C5:31) is inserted in a MAC table on the router. **NOTE:** Many devices that can connect to a wireless router may have two MAC address numbers; one for the LAN Ethernet port and another one for the wireless port (these are known as your device’s “network adaptors”). You want to use the wireless MAC address. Remember to also print all the MAC addresses with their corresponding device names (“Susie’s iPad XX:XX:XX:XX:XX:XX”). NOTE: This will stop the casual “drive-by” hacker, but not the determined attacker.

4. Change the router’s IP address as many routers (like Linksys/Cisco) use 192.168.1.1. as the default IP address. Since its a local connected device, just change one of the “1’s” to another number and that will work fine.

5. Change the **SSID** (Service Site Identifier) name to something not relating to your family name (my neighbor has “Trojan Horse”), then once you have configured those that **should** be connected with the wireless router (family but not neighbors). **NOTE: Turning your SSID “off” doesn’t stop identification (see next slide).**

6. Turn **OFF** the ability to ***remotely connect*** with the router to perform admin duties. What this means is that to perform admin duties you **MUST** be connected to the router via a hard-wire connect (Ethernet cable) to the device to make any changes. This thwarts those pesky hackers from connecting wirelessly into the router.

7. Set the connectivity type to **https**, vs. just straight http. Yes, it’s a little overkill, especially since the connectivity is via a locally connected hard-wire machine only, but adding another layer doesn’t hurt.

8. Remember to **Back-up** the settings (Cisco routers come with a USB port) for a flash drive.

9. Turn your router **OFF** at night or when gone from home. If your computers are off, so too the router. NOTE: Difficult to do if you are using the “internet of things.”

THE PARTNERS GROUP

Use a VPN

- Computers
- Tablets
- SmartPhones

THE PARTNERS GROUP

Use a Password Manager

keeper®

dashlane

LastPass****

StickyPassword

Options for ID Protection

Features	MyIDCare ID Experts	Lifelock Standard	ProtectMyID Experian
Monitoring Services: Single Credit Bureau and non-credit alerts	Yes	Yes	Yes
$1M of ID Theft insurance. Limit of stolen funds reimbursement	Yes up to $1M	Yes up to $25,000	Yes up to $1M
ID theft recovery assistance	Yes	Yes	Yes
Unique Features	Patented medical claims monitoring Alerts as employee benefit	Checking, Savings, Investment accounts alerts	Credit lock alerts
Retail monthly cost for An individual: A Family:	$9.95 $19.95	$9.99 N/A	$9.99 N/A

THE PARTNERS GROUP

How well do you know your business’ cyber exposures?

THE PARTNERS GROUP

What’s Your Company’s Risk?

1. Does your business retain physical or electronic records of the following?

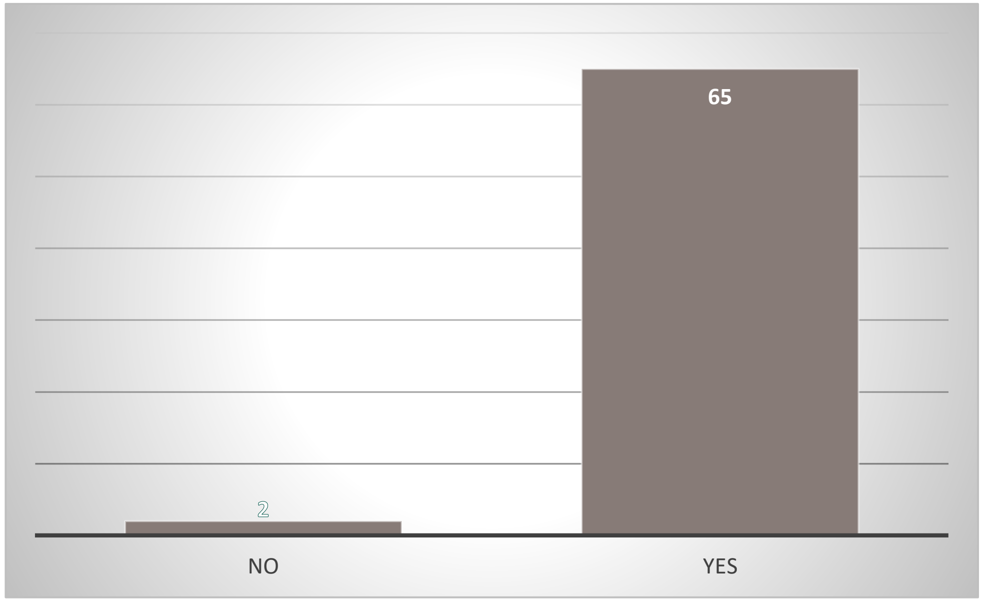
a. Social security numbers
b. Drivers’ license information
c. Tax identification numbers
d. Birth dates
e. Medical/health records
f. Court records
g. Police records
h. Banking information (checking/savings accounts)
i. Email addresses or home addresses

THE PARTNERS GROUP

What’s Your Company’s Risk?

1. Does your business retain physical or electronic records of the following—continued.

If you checked yes to any item on the previous slide, your organization is in control of “Personally Identifiable Information,” and therefore, required to protect that data subject to State and Federal privacy and data breach notification laws.



**TPG poll question results shown to the right

What’s Your Company’s Risk?

- **Does your business have employees?**

Many data breaches involve an employee mistake. They can lose a mobile device, laptop or paper records, or make costly errors such as opening an unauthorized email containing malware. In addition, they can even intentionally steal data.

THE PARTNERS GROUP

What’s Your Company’s Risk?

- **Does your business have an active website?**

Material posted electronically, or in written format, may lead to copyright or trademark infringement, or defamation litigation. If the website is transactional, additional exposures include possible hacking or disruption of your business via denial of service attacks.

What's Your Company's Risk?

- **Does your business use third-party vendors (e.g., cloud, IT services)?**

Businesses in possession of personally identifiable information may be held liable for privacy breaches caused by their vendors or other third parties. As the owner of the data, your business is ultimately responsible for protecting it.

What’s Your Company’s Risk?

- **Does your business accept credit card payments, other electronic payments or have online bill pay?**

Over 25% of all data stolen is credit card and other payment information. [1] This is a category of data that is highly desired by criminals for resale on the black market.

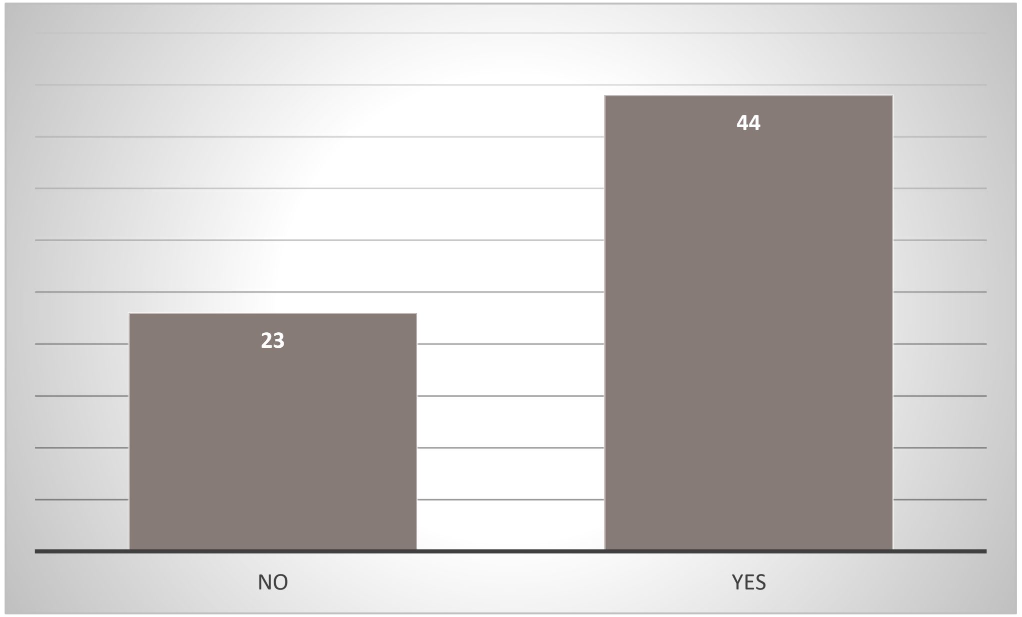
.

[1] *NetDiligence® 2015 Cyber Claims Study*

What’s Your Company’s Risk?

- **Does your business allow employees to use personal devices to connect to your network?**

Personal devices may not have the same security software and other connectivity procedures as company-provided devices. As a result, when these personal devices are connected to your network, there may be a higher exposure to virus or malware threats.



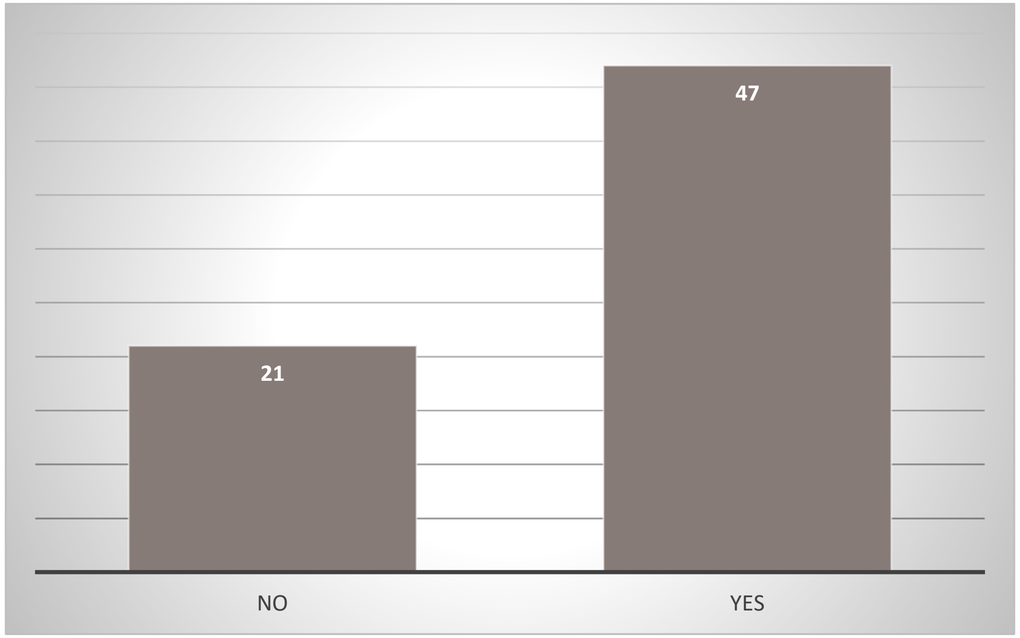
** TPG poll question results shown to the right

THE PARTNERS GROUP

What’s Your Company’s Risk?

- **Does your business train employees on proper email use and other privacy issues?**

Employee negligence and/or errors are one of the top three contributors of lost/stolen data. [2]



2. Ponemon Institute 2016 Cost of Data Breach Study
*** TPG poll question results shown to the right*

THE PARTNERS GROUP

What’s Your Company’s Risk?

- **Does your business store your customers’ corporate confidential information?**

Companies face liability for failing to protect their customers’ and business partners’ confidential information.

THE PARTNERS GROUP

Story by Numbers

55% of Small business owners experienced a cyber attack in the past 12 months [3]

14% of companies that rate their ability to mitigate cyber attacks as "highly effective“ [3]

47% of Data breaches caused by a malicious or criminal attack [4]

Accidental release of private data by an employee accounted for 25% of data breaches in 2016, while IT glitches and business process failures were the cause 28% of the time.

Source: Liberty Mutual - Cyber Risk [Infographic]. (n.d.). 175 Berkeley St, Boston, MA.
3. Symantec. Internet Security Threat Report Volume 22
4. Ponemon Institute. 2016 State of Cybersecurity in Small & Medium-Sized Businesses

THE PARTNERS GROUP

Cost of a Data Breach

- Forensic examination to determine scope
- Notification of affected customers and other parties
- Payments to a call center to handle customer questions
- Credit or identity monitoring
- Public relations
- Legal defense
- Regulatory penalties or proceedings
- Time element losses & loss or damage to data/property
- Liability for denial of service from or access to data

Cost of a Data Breach

The per record cost of a data breach averaged $141 in 2017. [5]

- Healthcare - $380
- Financial Services - $245
- Transportation - $123
- Services - $223
- Energy - $137
- Hospitality - $124
- Industrial - $149
- Retail - $154

5. Ponemon Institute. 2017 Cost of Data Breach Study

THE PARTNERS GROUP

Cost of Lost Business

While the average direct cost of data breaches is high, the cost of lost business can be much higher— more than $4.1 million on average. [6] These include:

- Abnormal customer turnover
- Increased customer acquisition costs
- Reputation loss
- Negative publicity
- Diminished goodwill

.

6. Ponemon Institute. 2017 Cost of Data Breach Study

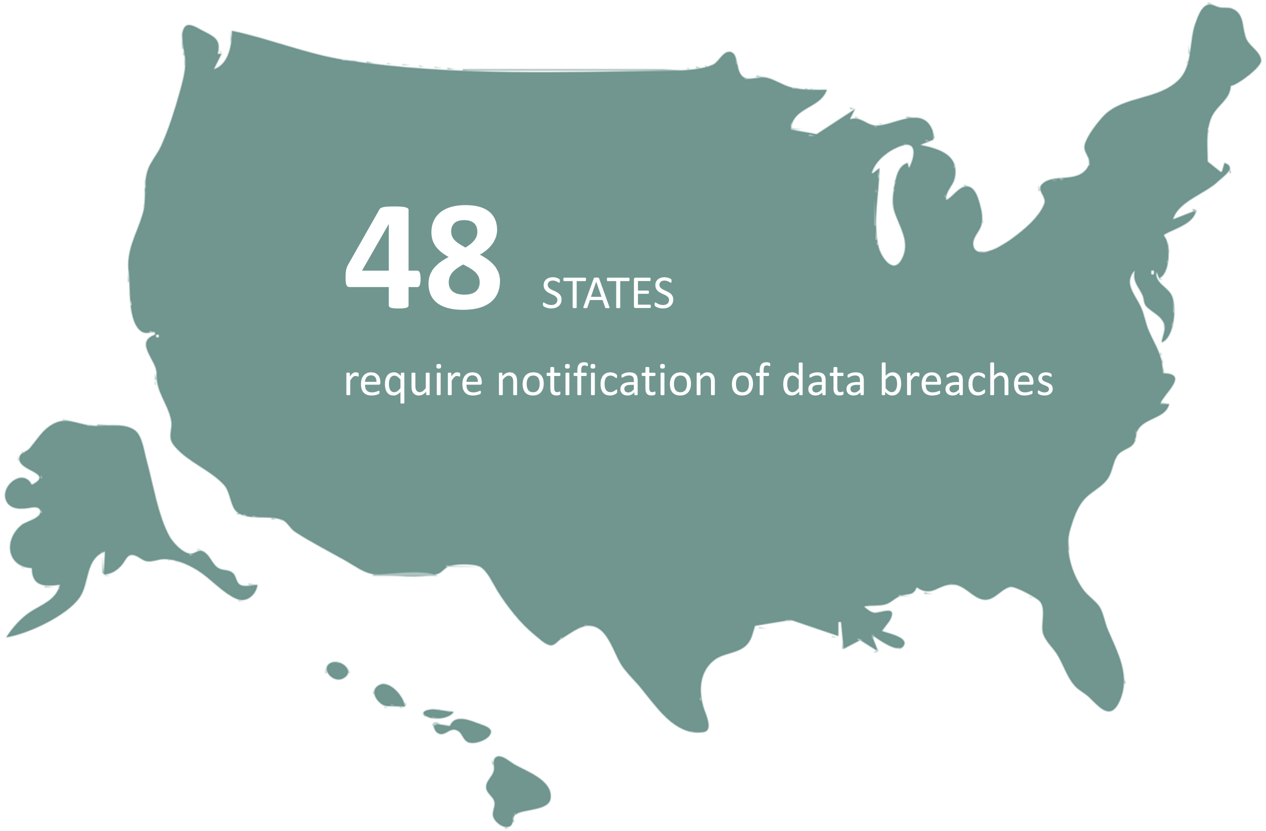
Risk of Attack

According to confirmed breaches in 2016, the likelihood of a cyber attack differs among industries and businesses. Here are four of the most vulnerable:

- Financial Services – 24%
- Retail – 15%
- Healthcare Organizations – 15%
- Public Sector Entities – 12%

7 Verizon. 2017 Data Breach Investigative Report

State Requirements



48 STATES

require notification of data breaches

Sample Coverage—Financial Loss

Third party loss resulting from a security or data breach

- Defense costs and damages if the business (or its outsourced handling firm) causes a breach of personal or corporate data
- Defense costs and damages if the business contaminates someone else's data with a virus
- Defense costs and damages if the business suffers theft of a system access code by non-electronic means

Sample Coverage—Financial Loss

Event management costs

- Costs of notification, public relations, and other services to manage/mitigate a cyber incident
- Expenses to restore, recreate, or recollect lost electronic data
- Forensic investigations, legal consultations, and identity monitoring costs for breach victims

Sample Coverage—Financial Loss

Network interruption

- Loss of net profit and extra expense as a result of a material interruption to the insured’s network caused by a security breach

THE PARTNERS GROUP

Sample Coverage—Financial Loss

Cyber/privacy extortion

- Ransom payments (extortion loss) to third parties incurred in terminating a security or privacy threat

Digital media liability

- Damages and defense costs incurred in connection with a breach of third party intellectual property or negligence in connection with electronic content

Sample Coverage—Tangible Loss

- Business interruption
- First party property damage
- Third party bodily injury and property damage
- Products/Completed Operations Coverage

Sample Consultancy Services

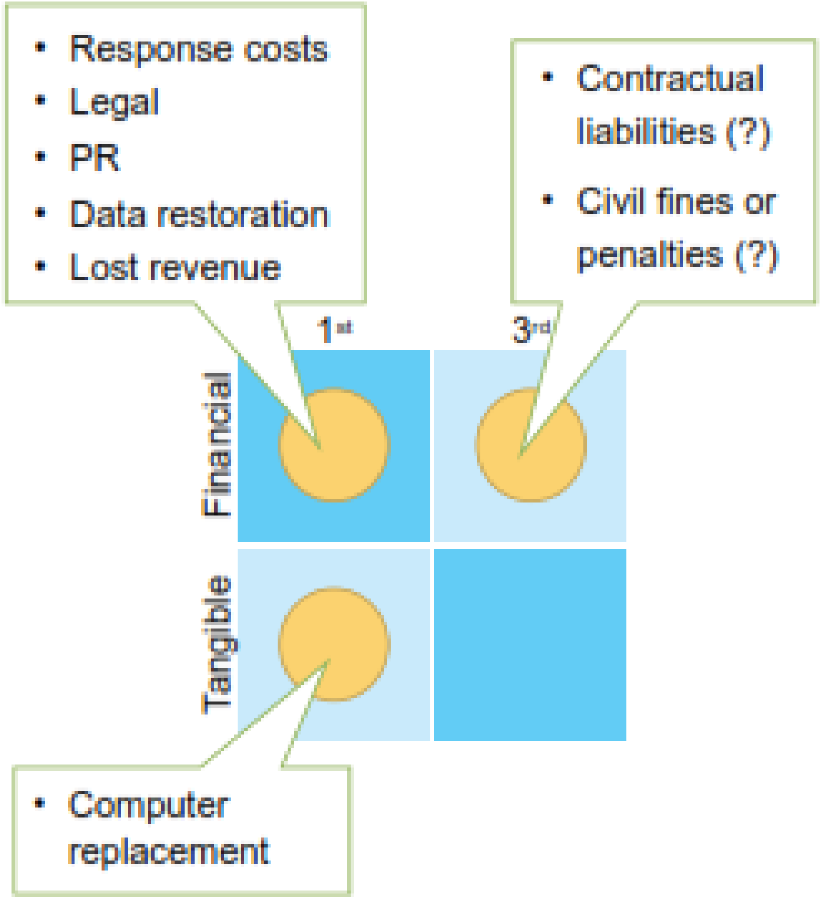
- Risk consultation and prevention before a breach
- IT consultancy for the business during and after a cyber breach
- Consultancy to safeguard and rebuild a company's reputation after a cyber breach

THE PARTNERS GROUP

Cost Grid Example

Property Damage & Business Interruption

Coordinated attack against an electric utility: Long term reconnaissance and multiple coordinated efforts involving spear phishing emails, malware, harvested credentials, and flooded call centers enabled attackers to manipulate the electric utility's SCADA system, causing a power outage for hundreds of thousands of customers.



- Response costs
- Legal
- PR
- Data restoration
- Lost revenue

- Contractual liabilities (?)
- Civil fines or penalties (?)

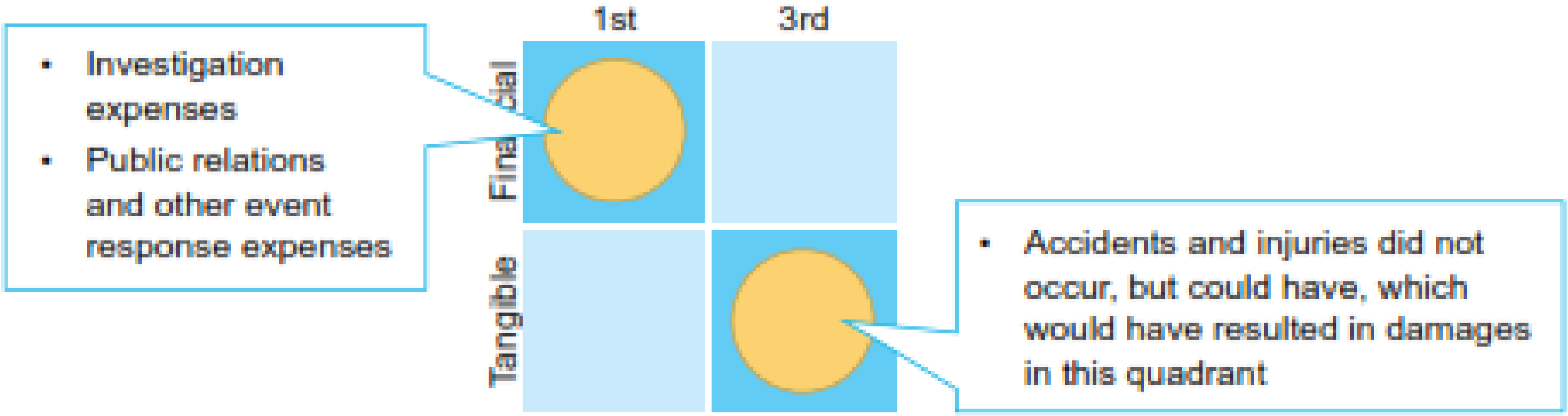
- Computer replacement

**AIG CyberEdge claim example

Cost Grid Example

Bodily Injury and Products/Completed Operations Coverage

Demonstrated ability to hack vehicles of major auto manufacturer: white hat hackers demonstrated their ability to remotely take control of a vehicle – no injuries resulted, but it demonstrated the potential for a cyber attack against products linked to the internet.



- Investigation expenses
- Public relations and other event response expenses

- Accidents and injuries did not occur, but could have, which would have resulted in damages in this quadrant

**AIG CyberEdge claim example

Actual Claim Examples

- An email server and external hard drive were stolen from the premises of an outside vendor. Personal information of approximately 175,000 individuals was compromised.

- The Insurance Company worked closely with the insured and provided reimbursement of $1 million for notification and the retention of professionals.

**AIG CyberEdge claim example

**AIG CyberEdge claim example

Actual Claim Examples

- An insured hospital was notified of a potential HIPAA breach involving protected health information (PHI) of over 40,000 patients.

- The Insurance Company quickly engaged with the insured to retain breach counsel and the further retention of a forensic investigator. Based on the ensuing investigation, they coordinated with the insured and breach counsel on the selection and retention of vendors to handle the required notification to regulators and patients, offered patients access to identify monitoring protection, and established a call center to handle inquiries and registration for the identity monitoring protection.
- Continued on next slide…..

THE PARTNERS GROUP

Actual Claim Examples

- The Insurance Company reimbursed the insured $450,000 for Credit Monitoring and ID Theft Insurance; $175,000 in notification and call center costs; $25,000 in forensic costs; and $90,000 in legal costs. The policy also covered $500,000 in regulatory fines assessed on the insured.

**AIG CyberEdge claim example

THE PARTNERS GROUP

Thank you

We will be distributing the PowerPoint, questions that have been posed during this presentation, and HRCI credit forms the week following this presentation.

THE PARTNERS GROUP