BREACHPRO

Brought to You by GLJ Benefit Consultants
Essential Law Firm Resources
DATA BREACH PROBLEM!!
“We’re not winning,” “I don’t see how we ever come out of this without changes in technology and changes in behavior” “We’re not winning,” Wall street Journal

FBI executive assistant director Shawn Henry
Data Breach Patterns!

Verizon 2014 Data Breach Investigations Report

Nine classification patterns covered the majority of security incidents.

In 2013, we analyzed over 63,000 security incidents and more than 1,300 confirmed breaches to provide new insight into your biggest threats and to help improve your defenses against them. This year’s report identifies nine basic patterns that covered 92% of all the 100,000 security incidents we’ve looked at from the past 10 years.
What’s On the Horizon?

2014 Security Predictions:

1. One Major Data Breach a Month – Erosion of Public Trust
2. Increased Cyber Kidnappings – Holding Data Ransom
3. Unsupported Software Attacks – XP, Java and others
4. Malware Gets Meaner and More Sophisticated – 60M
5. Network Attackers Become Cyber Shrinks – Behavior-Based
6. Continued Employee Mistakes – Lack of Policy's and Training
Threat to Law Firms!

Most major U.S. law firms have been victims of security breaches, and the unwelcome threats likely operated covertly for up to nine months before they were discovered. For many, the first whiff of insidious action comes from a knock on the firm’s door by the FBI.

In 2011, the U.S. government labeled New York City’s 200 largest law firms “the soft underbelly” of hundreds of corporate clients, two experts warned at a Tec show session on data security. Even midsize, boutique, and solo firms are at risk, warned presenters Sharon Nelson, president of information and digital technology firm Sensei Enterprises, and Ben Schorr, CEO of IT consulting firm Roland, Schorr & Tower. The untrained lawyers and office personnel are often the No. 1 chink in a law firm’s defense, the duo said.

“The biggest threat to law firms’ data are its own users, who aren’t trying to do damage,” said Schorr, who shared an anecdote of a firm that unwittingly allowed its receptionist access to read, edit and delete client documents. At another, an associate with Internet connection issues in his office used his own unprotected Wi-Fi router to work on client matters, WSJ
Threat to Law Firms!

On November 1, 2009, the FBI issued an advisory warning to law firms that they were specifically being targeted by hackers. Source ABA Journal
What is a Data Breach?

A data breach is the loss, exposure or theft of your customer’s or employee’s **Personally Identifiable Information** (PII)(PHI)(BII).

Examples of PII, PHI, BII:

- Full name
- Email address
- Social Security number
- Drivers License number
- Credit or debit card numbers
- Bank or other financial account numbers
- Medical or health records
How Breaches Happen?

43% Employee Mistakes!

- Employee error, mistakes
- Lost files, laptops, & flash drives
- Un-shredded files
- Unsecure electronic data disposal
- Disgruntled, ex-employees
How Breaches Happen?

33% Hackers/Criminals
- Computer, website hacking
- Spyware, viruses
- Phishing emails
- Key-loggers
- Social engineering
- Malware

24% System Glitches
- Hardware software conflicts
- Software bugs and glitches
The High Cost of Being Unprepared!

243 Days
Median # of days attackers are present on a victim network before detection.

3 months
6 months
9 months

Initial Breach
Threat Undetected
Remediation

Source: Mandiant M-Trends 2013

63%
of Companies Learned They Were Breached from an External Entity

100%
of Victims Had Up-To-Date Anti-Virus Signatures
US Data Breach Damages!

- $67 billion in damages per year since 2005
  Source (FBI)

- Over 744 million records lost or stolen since 2005

- $188-214 dollars per record
  Source (Ponemon Inst.)
Cost of Recovery?

DIRECT Costs:
- Customer Notification
- Investigation Expense
- ID / Credit Monitoring
- Crisis Management
- Legal/Civil Liability
- Regulatory Fines/Penalties
- Legal Defense Cost

IN-DIRECT Costs:
- Bad publicity/Goodwill
- Customer Loss
- Recovery Time

Targets customer data breach in December affected stock price drastically by almost 50%. Stock was around 85.50 a share by February 2014 stock was at 55.50 per share. With stock down and 1Billion dollars so far in regulatory penalties and fine. Target finds it's self with a fired CEO and lackluster profits for 2014. WSJ
“It takes 20 years to build a reputation...

...and 5 minutes to ruin it.”

Customers after a data breach:

- 40% will consider ending the relationship
- 30% will stop doing business
- 5% consider legal action  
  (CIO Magazine & Ponemon Inst.)

~Warren Buffett
Data Breach Summary

Top 4 Causes of Law Firm Data Breaches

- Improper Disposal of Records
- Theft, Loss of Mobile Device
- Misuse of Security Protocols
- Computer Hacking
## Breach Examples

<table>
<thead>
<tr>
<th>Date</th>
<th>Law Firm/Client</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 16, 2011</td>
<td>Law Office of Ashley Bell, Department of Family and Children Services, Gainesville, Florida</td>
<td>Sensitive client files were found in a newspaper recycling bin at The Gainesville Times. The files were related to the physical and sexual abuse of juveniles and client Social Security and phone numbers were exposed. The breach may have been caused by a college intern who disposed of the files inappropriately. Some files were as recent as 2009, but all cases were closed.</td>
</tr>
<tr>
<td>April 20, 2008</td>
<td>Law Office of Sole Practitioner</td>
<td>A thief stole a laptop from the car of a Baltimore sole practitioner that contained unencrypted information related to tax returns of clients. The attorney also stored personal data on the laptop related to any dependents whose names may have appeared on the tax returns.</td>
</tr>
<tr>
<td>January 2010</td>
<td>Morgan Keegan &amp; Company of Memphis</td>
<td>Confidential data. Despite having procedures in place to prevent unauthorized access, the internal protection systems were bypassed either through human error or duplicitous conduct. In January 2010, Morgan Keegan &amp; Company of Memphis produced to the Alabama Securities Commission client documents related to an ongoing multistate securities investigation. The documents contained SSN, ages, incomes, net worth, and other account info of Morgan Keegan clients. Morgan Keegan had received assurances prior to production that the data would be treated as confidential by the Alabama Securities Commission. In April 2010, An unredacted and redacted disk with the exhibits was delivered to the Alabama Securities Commission’s file room. 14 A plaintiff’s law firm could not access the Morgan Keegan data from the secure Web site and contacted the Securities Commission to get a copy of the order and the exhibits. The Commission inadvertently produced an unredacted copy of the exhibits to the lawyer for some of the investors who claim to have been harmed by Morgan Keegan. Morgan Keegan discovered the breach in September 2010 and provided notice later in September to its impacted customers. In addition, the Alabama Securities Commission conducted a detailed investigation of the incident and concluded that “the inadvertent copy of the disk was the result of the use of new technology(hyperlinks) in an administrative order for which long standing procedures failed to address all possible security concerns.”</td>
</tr>
<tr>
<td>November 2011</td>
<td>Fenwick &amp; West LLP</td>
<td>Fenwick &amp; West LLP, acknowledged that their firm has been breached twice by hackers. They noted that it is very unlikely that we are aware of most law firm data breaches since firms have a deeply vested interest in keeping breaches quiet. This may be less true in the future now that 46 states have data breach notification laws.</td>
</tr>
</tbody>
</table>
What is the Government Doing?

US Attorney General wants laws requiring notifications after data breach.

US Attorney General Eric Holder has asked Congress to create a federal law requiring that companies notify their customers after detecting serious intrusions. The law would also punish companies that either don't send a quick alert or haven't been doing enough to protect data in the first place.

The would-be law isn't strictly necessary when 46 states have notification requirements in place, but it would hold corporations to a similar standard across the country.
## Penalties & Fines

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLBA</td>
<td>Up to $100,000 for each violation. Business owners officers are personally liable for up to $10,000 per violation.</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Minimum of $100 per violation to a maximum of $1.5 million per year.</td>
</tr>
<tr>
<td>PCI</td>
<td>$10,000 in fines on the first violation, up to $500,000 per incident.</td>
</tr>
<tr>
<td>RED FLAGS RULE</td>
<td>Up to $3,000 per violation, plus attorneys’ fees.</td>
</tr>
<tr>
<td>ALA VIP</td>
<td>From $500 to $5,000 Per client record affected.</td>
</tr>
</tbody>
</table>
What is Industry Saying?

American Bar Associations 28 Suggestions

1. Have a strong password of at least 12 characters. 2. Don’t use the same password everywhere. 3. Change your passwords regularly. 4. Do not have a file named “passwords” on your computer. 5. Do not have your password on a sticky note under your keyboard or in your top right drawer. 6. Change the defaults on your wireless router and server. 7. Your laptop should be protected with whole disk encryption—no exceptions. 8. Backup media, a huge source of data leaks, should be encrypted. 9. Thumb drives, which are easy to lose, should be encrypted. 10. Keep your server in a locked rack in a locked closet or room. 11. Most smartphones write to memory make sure you have a PIN for your phone. Don’t use “swiping.” Also make sure that you can wipe data remotely. 12. Solos and small firms should use a single integrated product to deal with spam, viruses and malware. 13. Wireless networks should be set up with the proper security. First and foremost, encryption should be enabled on the wireless device. 14. Make sure all critical patches are applied. This may be the job of your IT provider, but too often this is not done. 15. If software is no longer being supported, its security may be in jeopardy. Upgrade to a supported version to ensure that it is secure. 16. Control access. Does your secretary really need access to all programs. 17. If you terminate an employee, make sure you kill the id, (including remote) 18. Do not let the former employee have access to a computer to download personal files with- out a trusted escort. 19. Using cloud providers for software applications make sure reasonable inquiry is done into their security. 20. Be wary of social media applications, as they are now frequently invaded by cybercriminals. 21. Consider whether you need cyber insurance to protect against the possible consequences of a breach. 22. Have a incident response policy. 23. Let your employees know how to use social media as safely as possible, and if an incident happens, it is helpful to have a plan of action in place. 24. Dispose of anything that holds data, including a digital copier, securely. For computers, you can use a free product like DBAN to securely wipe the data. 25. Make sure all computers require screen saver passwords, and that the screen saver gets invoked within a reasonable period of inactivity. 26. Use wireless hot spots with great care. Do not enter any credit card information or login credentials prior to seeing the https: in the URL. 27. For remote access, use a VPN or other encrypted connection. 28. Do not give your user id and password to anybody. None of these safeguards are hard to implement. Unfortunately, even if you implement them all, new dangers will arise tomorrow. The name of the game in information security is “constant vigilance.”
solution
The BreachPro Suite

Prevent Compliance Issues with

Protect Your Systems with

Preserve Your Assets with

InfoSafe CERTIFIED

FireEye

beazley

BREACHPRO

ALA VIP Value in Partnership
How Does BreachPro Do It?

Manage the risk Prevent, Protect, Preserve

- Risk Assessment - Prevent, Protect, Preserve
- Compliance Program Administrator
- Information Security Policy
- Employee Training
- Physical Safeguards
- Vulnerability Assessments
- Technical Safeguards
- Breach Response Plan
Prevent Compliance Issues with InfoSafe CERTIFIED
InfoSafe®
Your roadmap to privacy and information security compliance.

My Compliance Program

- Find out **where you are at risk** of having a data breach
- **Protect** your confidential customer, employee, and business information.
- **Get compliant** with federal, state and industry regulations for safeguarding against data theft or accidental exposure including HIPAA, GLBA, Red Flags Rule, PCI DSS and more.

**Your InfoSafe program includes:**
1. Risk assessment
2. Custom information security policy
3. Training
4. Implementation tools
5. Compliance documents & resources
Set Up My Compliance Program

Step 1 - Risk Assessment

Overview

About the Risk Assessment: The first step in getting on the road to compliance and protecting your confidential data is to do a complete risk assessment for your business. This is a comprehensive risk assessment with detailed questions about your business and your current information security and privacy practices. The objective is to help you identify the information security vulnerabilities in your business including physical security risks, technical safeguards and administrative safeguards (people and paper processes). Your answers are used to create your Information Security Plan, training program, and your compliance implementation checklist.

Instructions: The person completing this risk assessment is typically the company's assigned Compliance Program Administrator. Please answer the questions in order, by section, as accurately as possible. You may need to consult other individuals in your organization for some answers. You can stop anytime during the assessment and return to complete later. Be sure to SAVE your answers in each section before moving on.

Print Entire Assessment: You may choose to download/print the entire risk assessment or some of the sections individually and complete it on paper before completing the assessment online. Be sure to SAVE your answers before exiting.

Compliance Requirement: Doing a complete risk assessment like this on a regular basis (at least once a year) is a requirement in order to stay compliant with the various regulations your business must follow.
1. Name of Company: ___________________________ Name of Applicant: ___________________________
   (as it would appear on a policy Please Print)

   Physical Address: ___________________________

   City: ___________________________ State: _______ Zip Code: _______

   Phone: ___________________________ Email: ___________________________

   Web Site: ___________________________ No. of years in business _______ No. Employees _______

   Is your company a:  □ Corporation  □ Partnership  □ Individual  □ LLC  □ Other

2. Type of Business/Services Offered: ___________________________

3. Total Yearly Gross Revenue: ___________________________

4. Total Approximate Number of Records Stored: ___________________________

5. Does your network have firewall protection that is securely configured?  □ Yes  □ No

6. If you store personal information on portable devices, is such data encrypted to industry standards?  □ Yes  □ No

   Check here if you do not allow employees to download personal/confidential information to portable devices.  □

7. Does your company use anti-virus software on all desktops, portable devices & servers  □ Yes  □ No
1.0 Introduction

Completed for:

On May 2, 2012, at 7:01 PM, an External Vulnerability Assessment was conducted by an InfoSafe technician with INVISUS. This is a penetration test of your Internet connection (IP address) of your business location and/or your website to determine if you currently have known security vulnerabilities.

This report shows specific vulnerabilities discovered that should be resolved in order to be compliant with the best practices commonly found in government and industry regulations such as PCI compliance. Vulnerabilities detected through this test may potentially be exploited by hackers to gain access to your computer systems, websites, customer databases and other private business and financial information.

(This is an external assessment only and does NOT check for internal security vulnerabilities such as malware and hacker tool infections, security patch updates and other security settings on your computers, servers or any wi-fi internet connections.)

Categories of Vulnerability:

CRITICAL PROBLEMS

Vulnerabilities which pose an immediate threat to your network by allowing a remote attacker to directly gain access to your network and/or computers on the network. These also can allow an attacker to perform a Denial of Service (DoS) which would take down your access to the internet.

AREAS OF CONCERN

Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

POTENTIAL PROBLEMS

Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. These may not pose an immediate threat to the integrity of your network, but may allow an attacker to gain information which can lead to threats.

2.0 Vulnerabilities by Severity

This section shows the overall number of vulnerabilities and services detected at each severity level:

- Critical: 10
- High: 7
- Medium: 2
- Low: 3
- Informational: 2

3.0 Overview

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

3.1 Host List

This table presents an overview of the hosts discovered on the network:

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Notice Name</th>
<th>IP Address</th>
<th>Host Type</th>
<th>Critical Problems</th>
<th>Areas of Concern</th>
<th>Potential Problems</th>
<th>PCI Compliant?</th>
</tr>
</thead>
<tbody>
<tr>
<td>wp.cpt.70-168.213-164.ph.l.c.com</td>
<td>70-168.213-164</td>
<td>Linux 2.6.16</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>FAIL</td>
<td></td>
</tr>
</tbody>
</table>

3.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network:
Internal Vulnerability Reports

Monitoring Report for Example Agency.
Report Date: 2/18/2014

 Workstation 1
22 Missing Patches, 6 Vulnerabilities Identified

- Update for Windows 7 for x64-based Systems (KB27256535)
- Update for Windows 7 for x64-based Systems (KB2773072)
- W8KFU 11.0.1 x64
- Update for Windows 7 for x64-based Systems (KB78946049)
- Internet Explorer 10 for Windows 7 for x64-based Systems
- Malwarebytes AntiMalware 1.75.8.1.1006
- Service Pack 2 for Microsoft Office 2010 (KB2674155) 32-Bit Edition
- Update for Root Certificates for Windows 7 for x64-based Systems (November 2013) (KB9931125)
- Update for Windows 7 for x64-based Systems (KB2830477)
- Google Picasa 3.9.137.81

Potential Vulnerabilities

Open port commonly used by Trojans: TCP 623 - LMS.exe
Open port commonly used by Trojans: TCP 2022 - LogMeln.exe

AutoShareW6S
The administrative shares (C$,D$,ADMIN$,etc) are available on this machine. For Internal networks these are normally turned on for administrative purposes. For Web server(s) these are normally turn off to in order to harden the possible entry points (since it is more exposed to attacks.). If you don’t use them set HLM\SYSTEM\CurrentControlSet\Services\LanmanServer\parameters\AutoShareWS to 0 to prevent creation of these shares. For more information, visit: http://support.microsoft.com/support/kb/articles/Q225/1/17.asp

AutoShareWKS
The administrative shares (C$,D$,ADMIN$,etc) are available on this machine. For Internal networks these are normally turned on for administrative purposes. For Web server(s) these are normally turn off to in order to harden the possible entry points (since it is more exposed to attacks.). If you don’t use them set HLM\SYSTEM\CurrentControlSet\Services\LanmanServer\parameters\AutoShareWS to 0 to prevent creation of these shares. For more information, visit: http://support.microsoft.com/support/kb/articles/Q225/1/17.asp

Cached Logon Credentials
Microsoft Windows NT caches the logon information of users who would have logged on, so that they would be able to logon when the server is unavailable. When a domain controller is unavailable and a user’s logon information is cached, the user will still be allowed to logon. The cache can hold up from 0 to 50 logon attempts, with the value of 0 disabling logon caching. If the value is set to a high value and an administrator logs in to computers to solve specific problems, an attacker might obtain the credentials of the administrator at a later stage, and logon with such an account, having powerful privileges. The registry value for setting this type of caching is: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonCount. Ideally it should be set to either 0 to disable caching, or else it should be set to 1 to provide for functionality (allowing the last user to logon immediately next time) and security.

Shutdown without logon
Anybody is allowed to shutdown this computer. For more information, visit: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp559.asp
Vulnerability & Monitoring Reports!

<table>
<thead>
<tr>
<th></th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
<th>Sun</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive Space Change Check - drive C:</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Drive Space Change Check - drive D:</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Exchange Store Size - SBS-MAIN\Mailbox Store (SBS-MAIN)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Exchange Store Size - SBS-MAIN\Public Folder Store (SBS-MAIN)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Hacker Check</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
</tbody>
</table>

(Last Response 03 Mar 2013 15:14 PM)

- Total: 39.06GB, Free: 14.68GB, Change: 0.00%
- Total: 62.68GB, Free: 25.50GB, Change: 0.00%
- Store size: 8.00MBytes
- Store size: 22.00MBytes

1,485 Attempts

Hacker Attempts Per Week

1,485
Protect Your Systems with FireEye™
Company Overview

- 2000+ Employees in 6 Continents, with HQ in Milpitas, CA.
- 1600+ Customers, in every region, every industry.
- Named David Dewalt as FireEye CEO 11/2012
- Over 100% Revenue Growth, over $100m in bookings in 2012.
- Recently launched on NASDAQ Stock Exchange under symbol FEYE, 100% share value growth in opening trading.

Deloitte. Technology Fast 500™
Number 1 Fastest Growing Network/Communications Company

2012 Technology Innovation Award
Inducted into Hall of Innovation
FireEye Platform Advantage

- Multi-Flow Analysis
- Multi-Vector Analysis
- Cross-correlated Intelligence
- Bi-directional Cloud Sharing
- Time to Protection

Thousands of Permutations (files, OS, browser, apps)

Web
Email
File
Mobile

Dynamic Threat Intelligence Cloud

Real Time Private Scalable Cross-Enterprise

BREACH PRO

Value in Partnership
Preserve Your Assets with BreachPro Insurance Partners
Our Insurance company’s of specialist insurance businesses have operations in Europe, the US, Asia, and Australia.

- In 2013, underwrote gross premiums of $1,970.2 million.
- All Lloyd’s Syndicates are rated A (Excellent) by A.M. Best and also benefit from the Lloyd’s chain of security.
- Clients:
  - Over a quarter of the American top 200 list of firms in the US

Breach Response (BR) – Cyber Liability Product

- BR is a unique insurance, loss control, and risk mitigation service that provides a comprehensive service to notify and protect customers of policyholders that have suffered a data breach.
- Handled more than 1,200 breaches since 2007.
  
  Retention rate >95% for customers who have experienced a breach.
## Cyber Liability Data Breach Insurance

<table>
<thead>
<tr>
<th>Coverage Provided</th>
<th>Benefits Offered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach response services provided outside the limit of liability</td>
<td>Notified individuals offered 12 months of free 3-bureau credit monitoring</td>
</tr>
<tr>
<td>Forensic and legal assistance from panel of privacy experts</td>
<td>Regulatory defense and penalties coverage up to $1,000,000</td>
</tr>
<tr>
<td>Notification provided on number of affected individual basis, not a capped dollar amount</td>
<td>Public relations and crisis management expenses up to $250,000</td>
</tr>
<tr>
<td>Coverage included for Cyber Extortion</td>
<td>1&lt;sup&gt;st&lt;/sup&gt; Party Coverage Endorsement provides coverage for business income and data restoration</td>
</tr>
<tr>
<td>Identity theft fraud resolution services for individuals enrolled in credit monitoring who become victims of identity theft</td>
<td>Free loss control information service provided with each policy, including compliance and breach response information, email alerts of key legal and regulatory developments, and expert online support for client questions on data security issues</td>
</tr>
</tbody>
</table>
BreachPro Includes

✓ Website Resources
✓ Education Experts
✓ Compliance Consultants
✓ Insurance Professionals
✓ Response Teams
✓ Training Teams
✓ Legal Defense Teams
✓ 30 Day Risk Free Trial
Thank You!

Next Step

Secure Your Law Firms Future!

All content in this presentation is copy written by GDSS / BREACHPRO / and partnering affiliates. This presentation and it’s contents can not be used reproduced or duplicated in anyway only upon written notice of copy write holder.