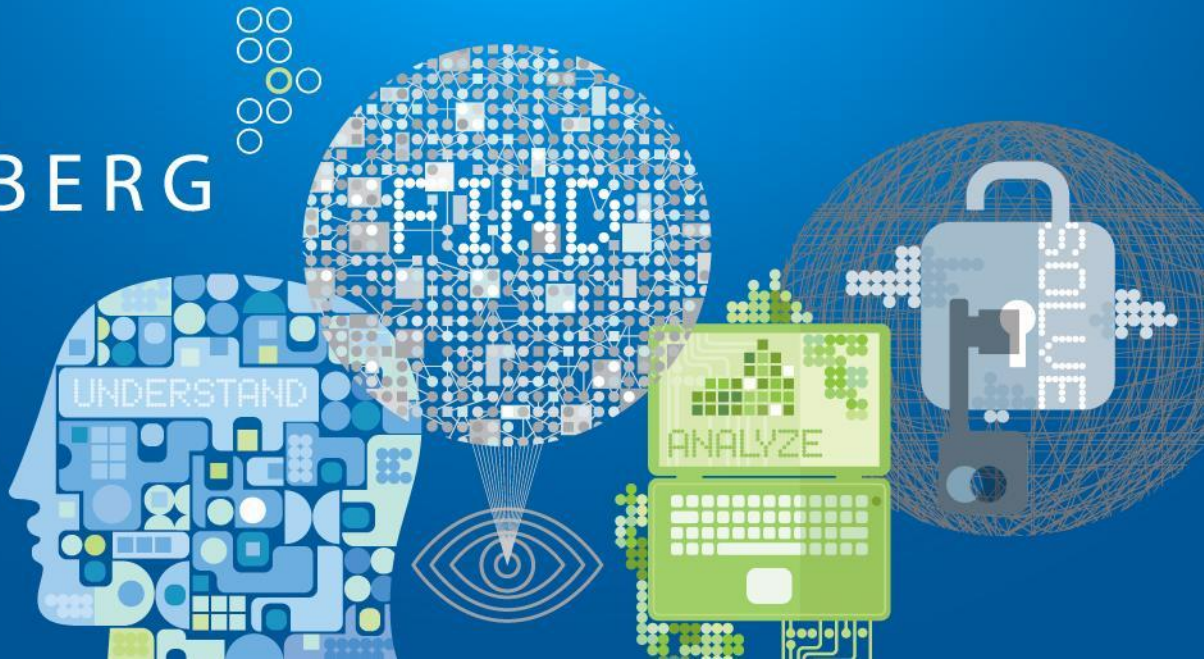
STROZ FRIEDBERG



Data Breach Strikes - Nerds & Geeks Unite:

Effective Cooperation Between Privacy and Technical Experts

Presented by:

Paul H. Luehr, Managing Dir.
Stroz Friedberg

Gerard M. Stegmaier, Esq.
Wilson Sonsini Goodrich & Rosati

Data Breach Trends

2011 Average Loss to Organization = $5.5 million

- Down from $7.2 million in 2010
- Not including organizations in excess of 100,000
- Low of $566K, High of $20.9 million

2011 Average Loss per Victim = $194

- Cost per Malicious Attack = $222
- Cost per Negligent Employee = $174

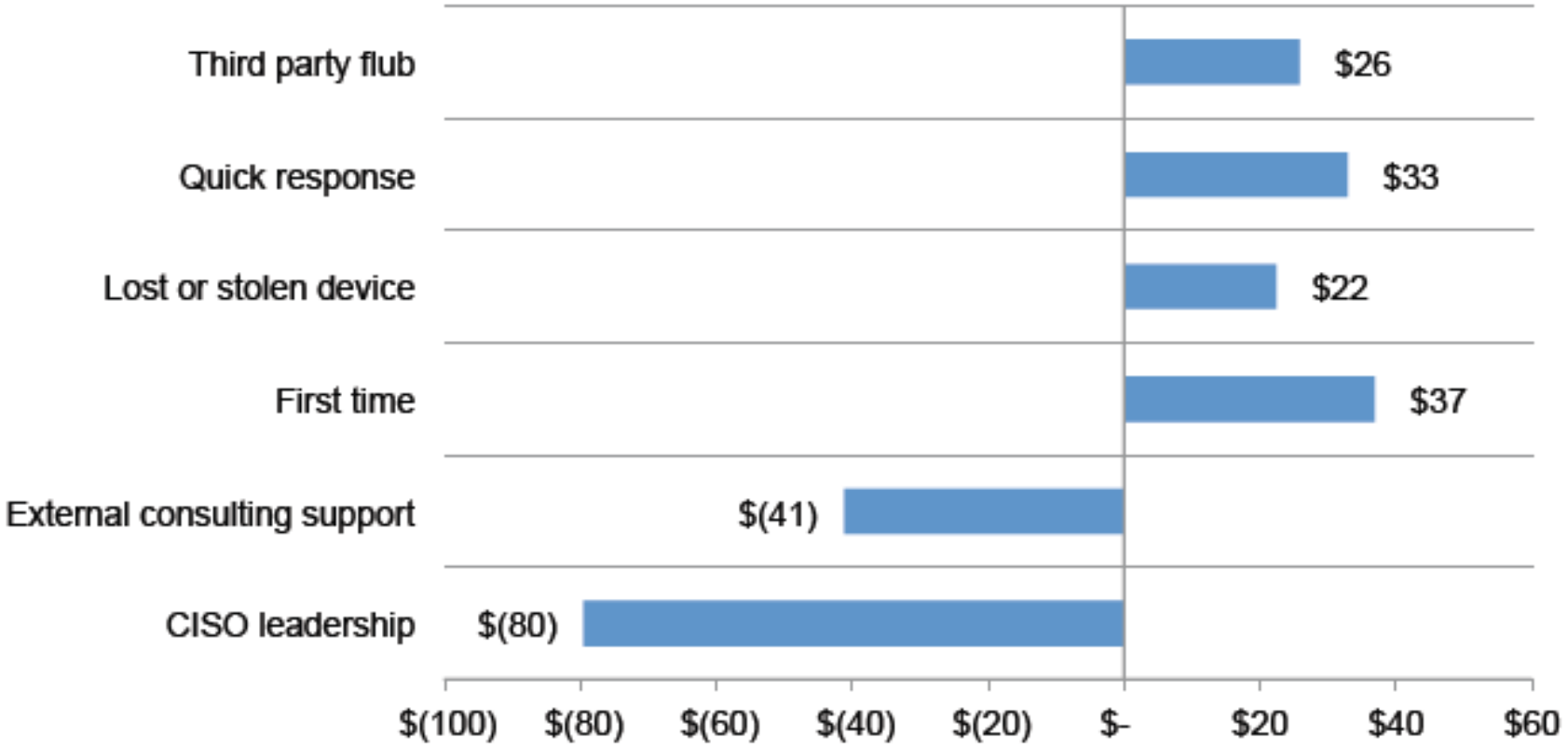
2011 Malicious Attacks, up over 3x

- Up from 12% to 24% to 31% to 37% (2008-2011)

Source: Ponemon Institute/Symantec, **2011 U.S. Cost of a Data Breach Study** *(49 organizations across 14 sectors)*

Data Breach Trends

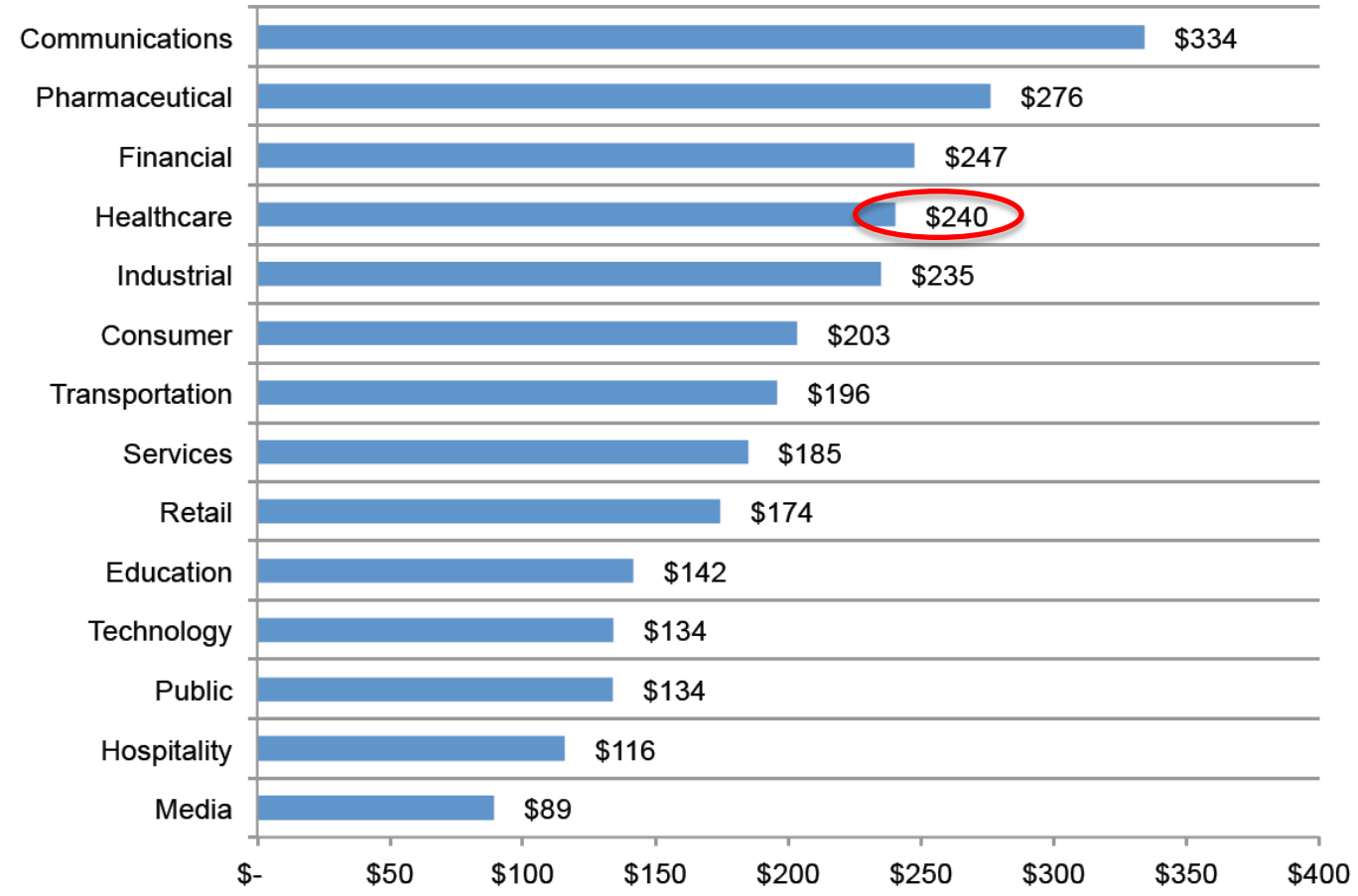
Figure 10. Per capita cost differences for six attributes or conditions



Source: Ponemon Institute/Symantec, **2011 U.S. Cost of a Data Breach Study**

Data Breach Trends

Figure 4. Per capita cost by industry classification of benchmarked companies



Source: Ponemon Institute/Symantec, **2011 U.S. Cost of a Data Breach Study**

Data Breach Trends – Health Care

96% of Health Companies Surveyed had a Breach

- Average of 4 over past 2 years
- 46% had more than 5 in past 2 years

$2.2 million = Average Financial Impact

- Up 10% from 2010

Discovered through:

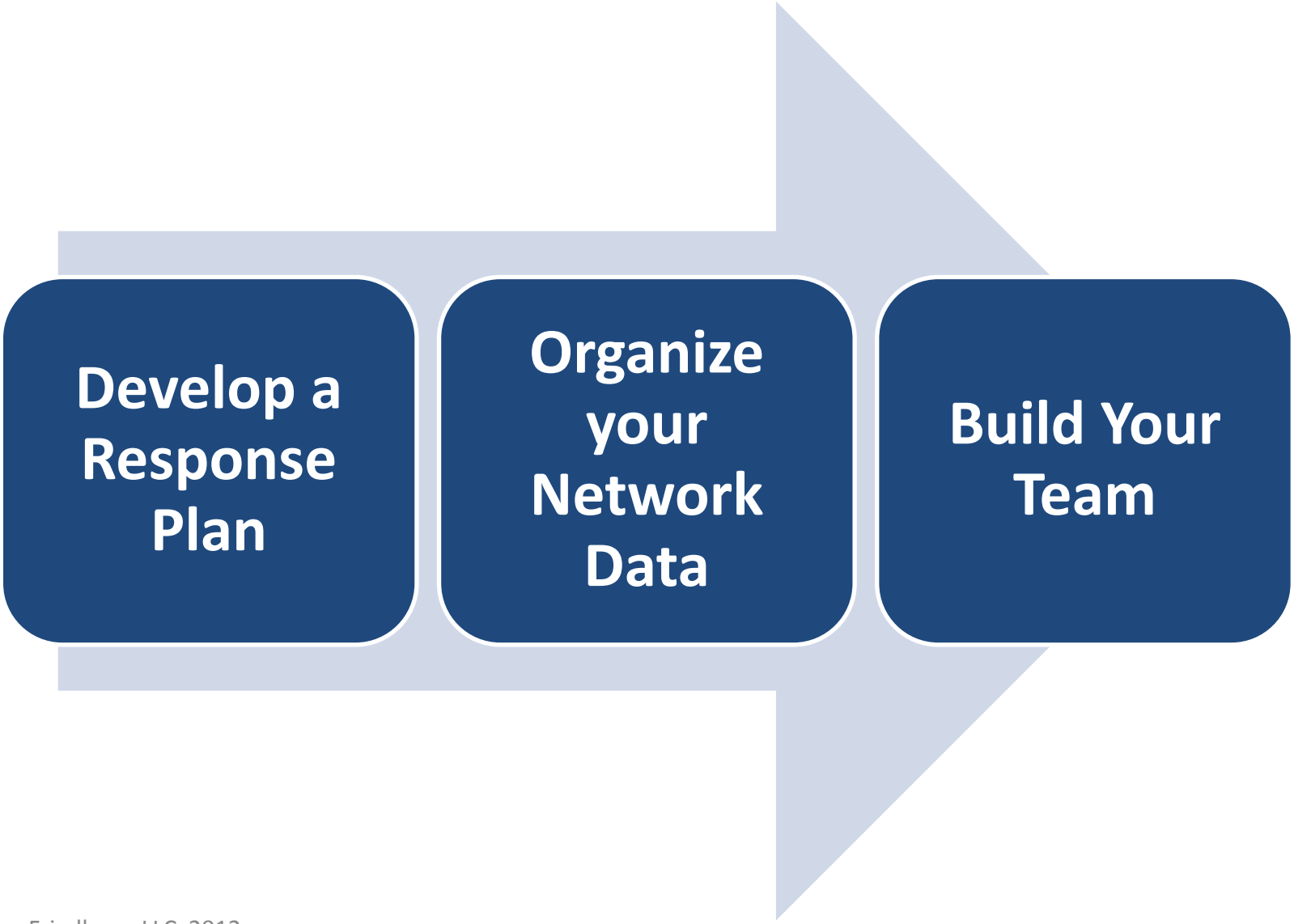
Employees (55%), Audit (45%), Patients (35%)

Source: Ponemon Institute/ID Experts, **2nd Annual Benchmark Study on Patient Privacy and Data Security** *(2011)(72 organizations surveyed)*

Responding to Data Breaches

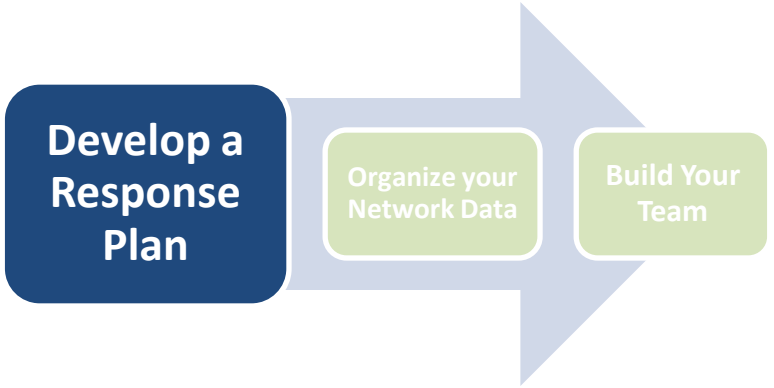
PREPARE
PRESERVE
SEARCH
ASSESS
COMMUNICATE

PREPARE for Disaster



PREPARE: Develop a Plan

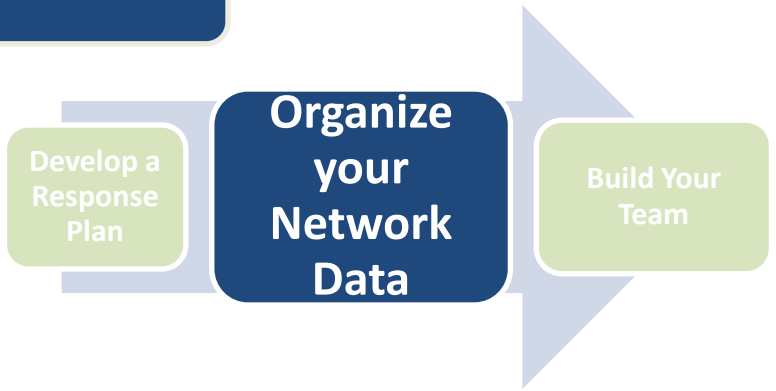
- Management endorsement
- Contact Lists
- Legal Analysis and Timeline
- Categories of adverse events
- “First steps” checklist
- Facilities and equipment lists
- Outreach plan



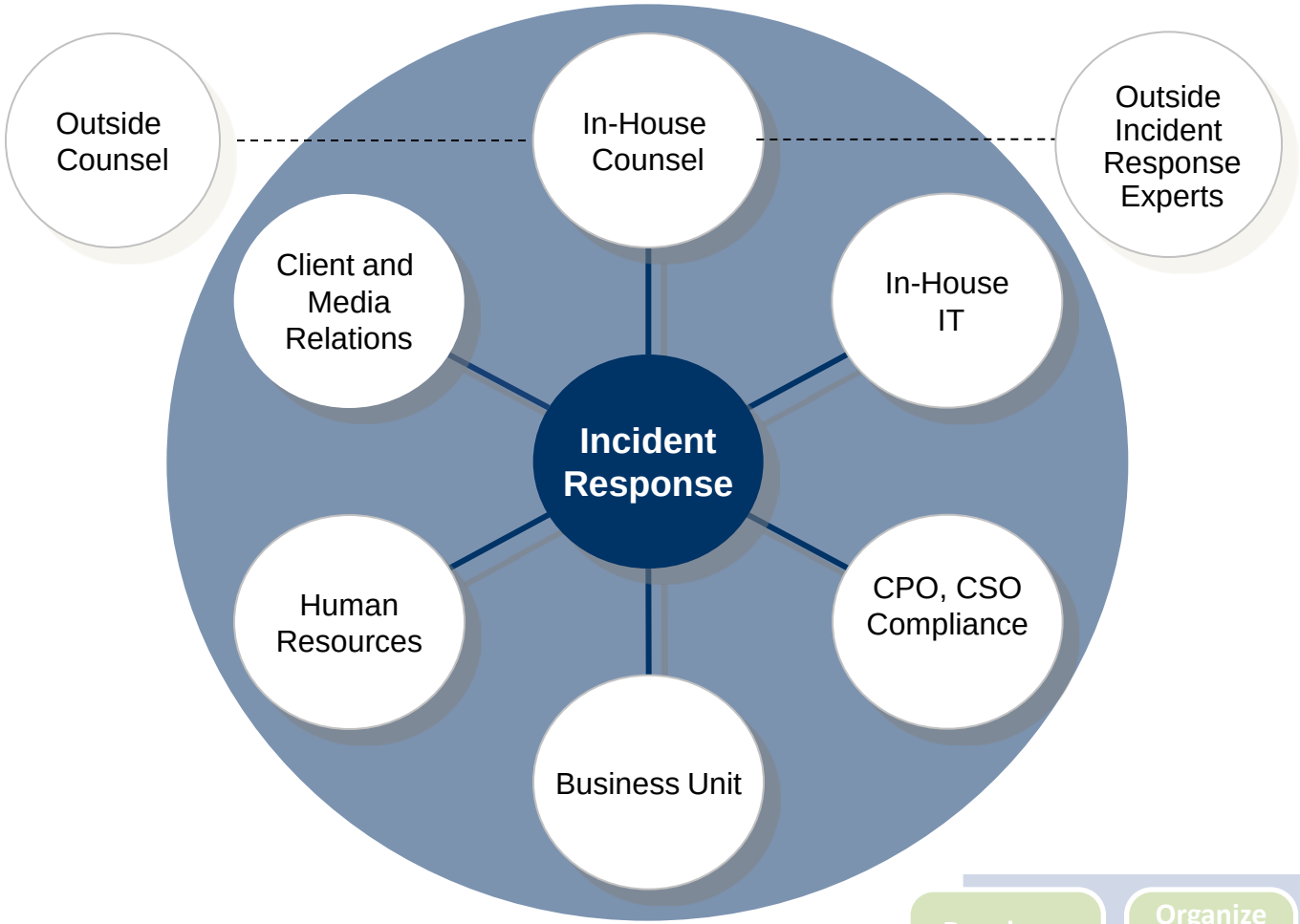
PREPARE: Organize your Data

- Map your critical assets
- Record backup schedules and inventories
- Update user lists
- Centralize logging functions
- Synchronize network times

"Where's your stuff?"



PREPARE: Build your Team



Develop a Response Plan

Organize your Network Data

Build Your Team

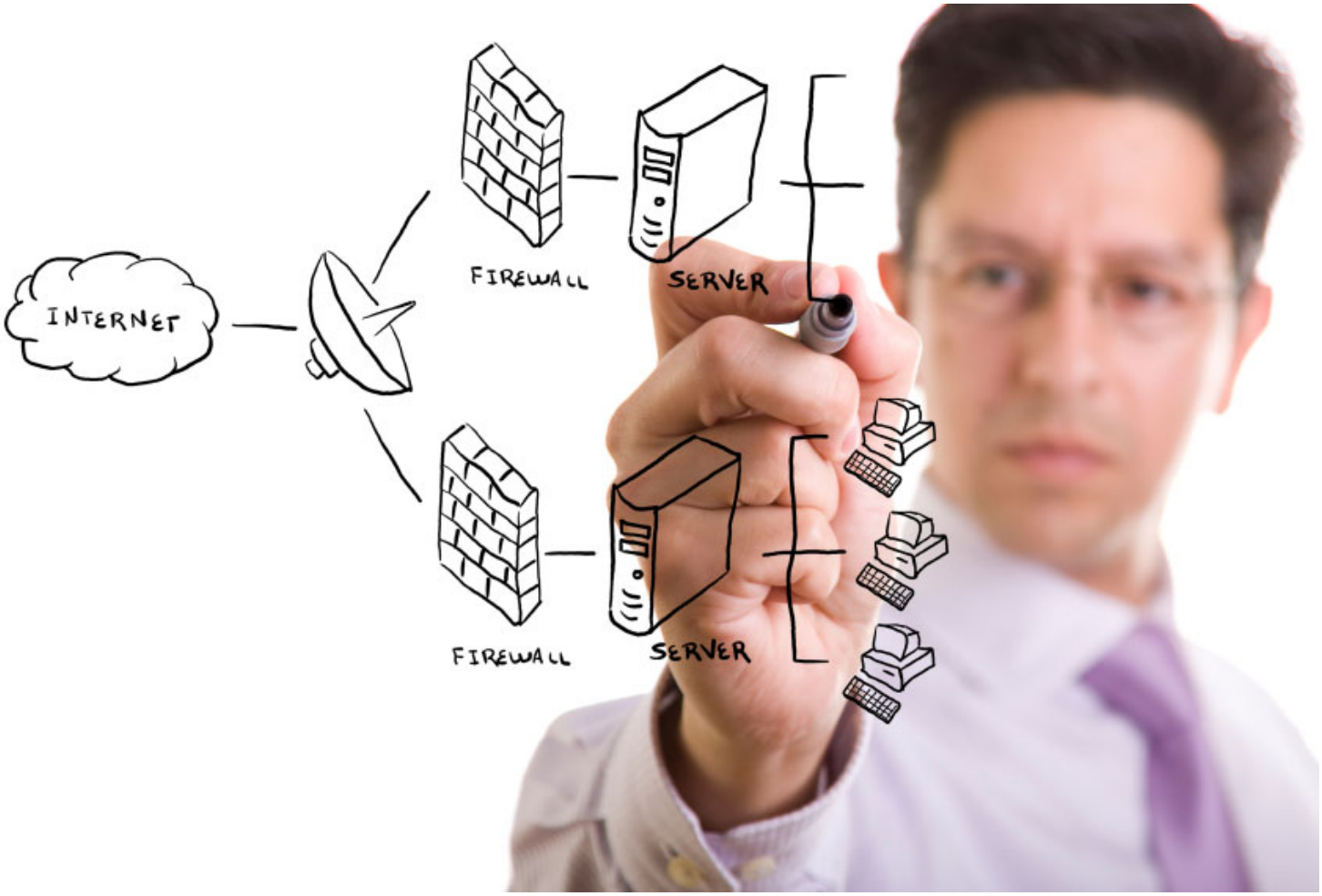
Data Breach – Types

Examples:

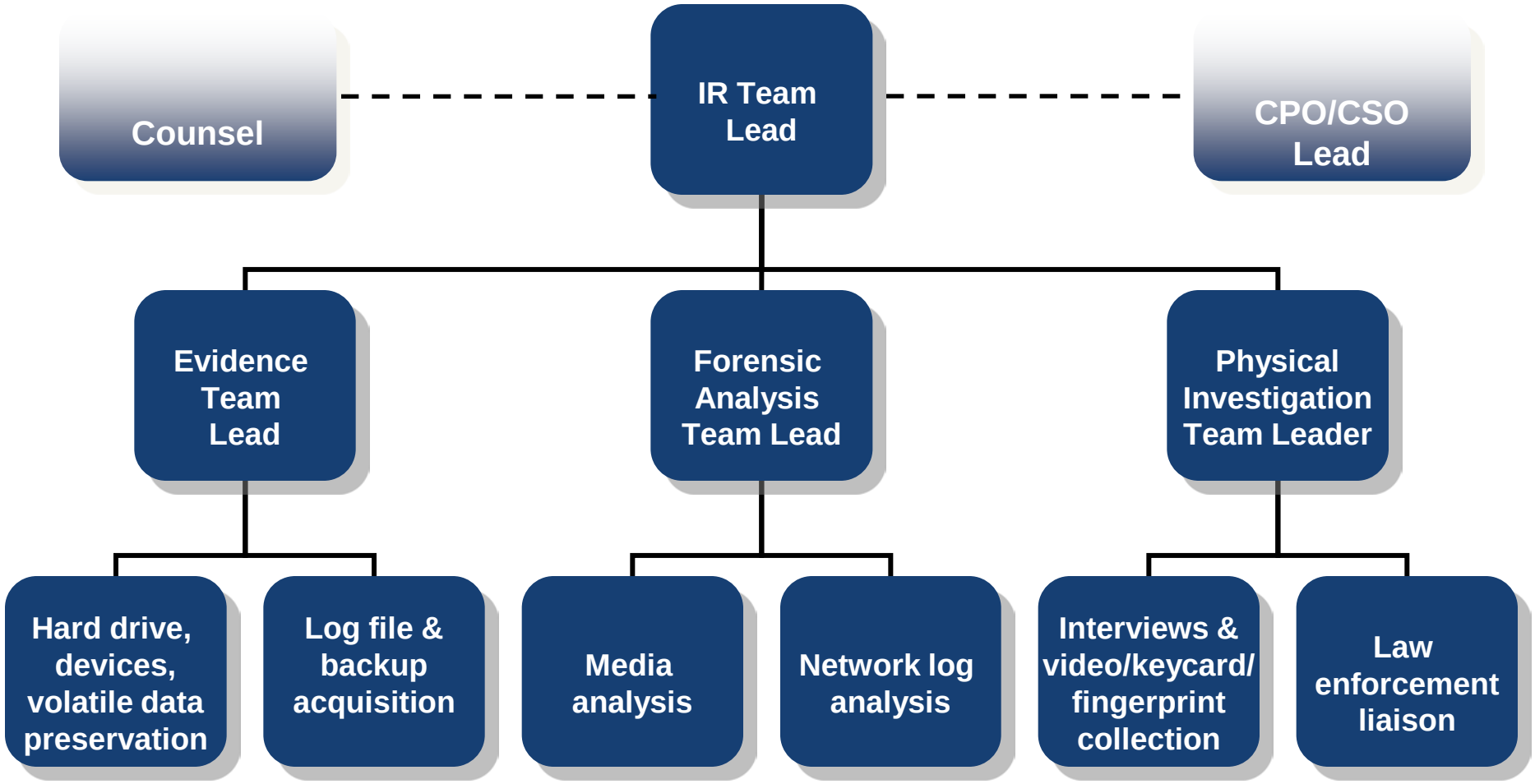
- **Hacking**
  - Phishing/spear phishing
  - Brute force attack
  - SQL injection
  - Advanced Persistent Threat (APT)
- **Data theft or loss**
  - Media stolen (e.g. laptops, thumb drives, tapes)
  - Data stolen (e.g. by current or former employee)
  - Data lost (e.g. in taxi or during data migration)
- **Data leakage**
  - Exposure to public (e.g. via web site)
  - Exposure to unauthorized person (e.g. wrong employee)
  - Sensitive data sent via unencrypted channel

Data Breach – Vectors

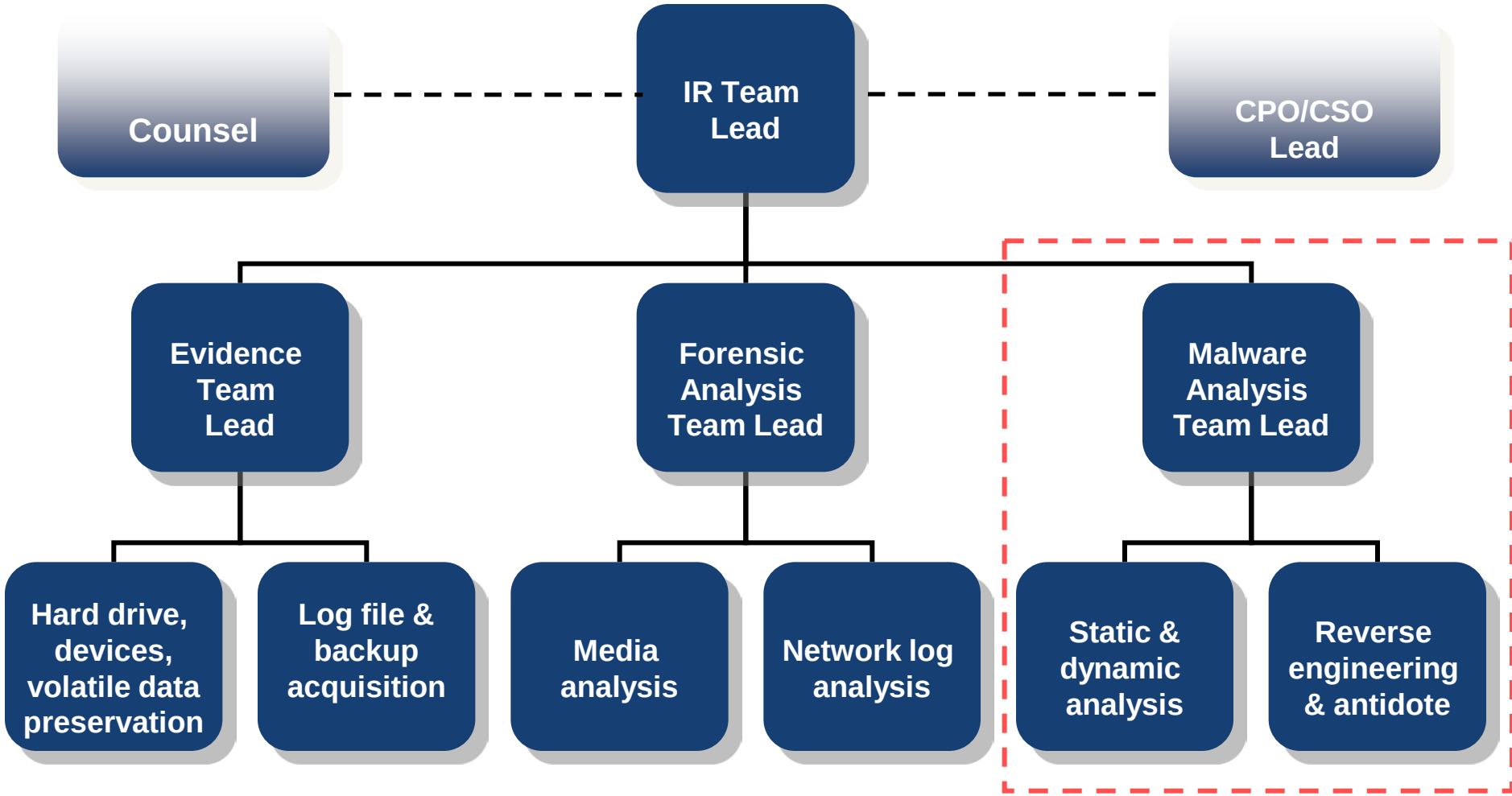
External **Internal**



Response Team (Internal Threat)

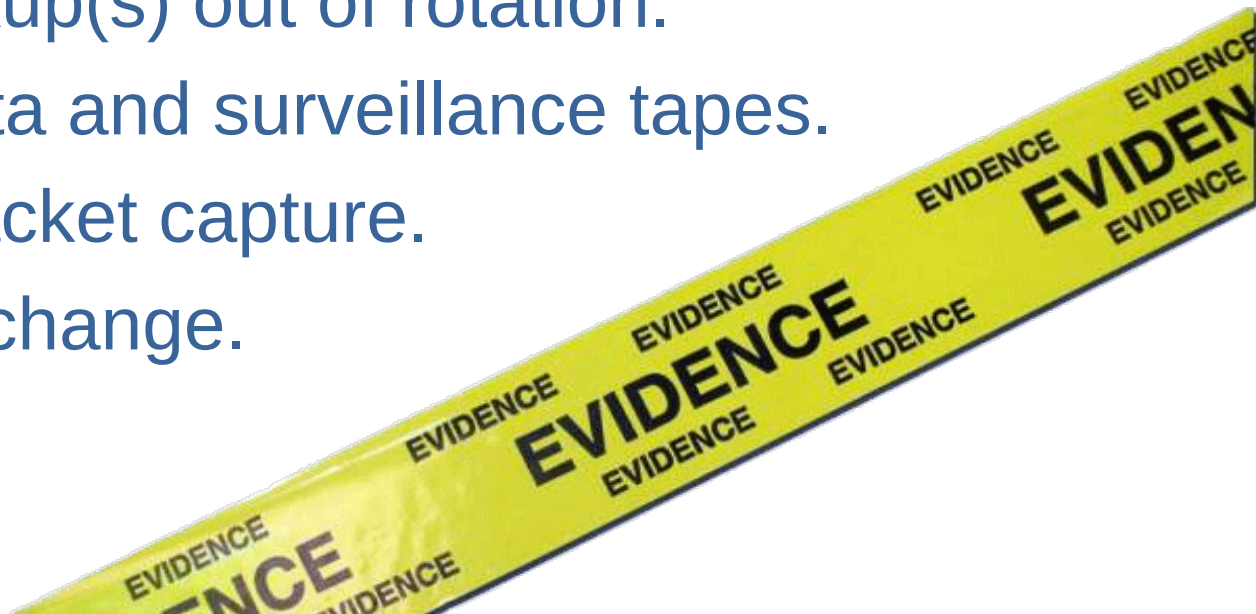


Response Team (External Threat)



PRESERVE the Data

- Unhook infected machines (leave power on).
  - Do **NOT** poke around.
  - Insert clean and patched machines.
- Call forensic experts to image infected machines.
- Save off log files (e.g. web, firewall, IDS).
- Pull needed backup(s) out of rotation.
- Save keycard data and surveillance tapes.
- Start real-time packet capture.
- Force password change.



PRESERVE - Challenges

Coordinating IT and Forensic Activity

- **IT needs to secure data environment**
  - Pull network connection, save backups and logs, prepare clean “builds,” force password change, update antivirus
- **Forensic needs to review active/latent data**
  - Image servers and report findings

Business Continuity

- **Migrate data after forensic imaging**

SEARCH and ASSESS – Internal Threats

SEARCH and ASSESS – Internal Threats

Internet Activity

Banking activity

Employment activity

Internal server access

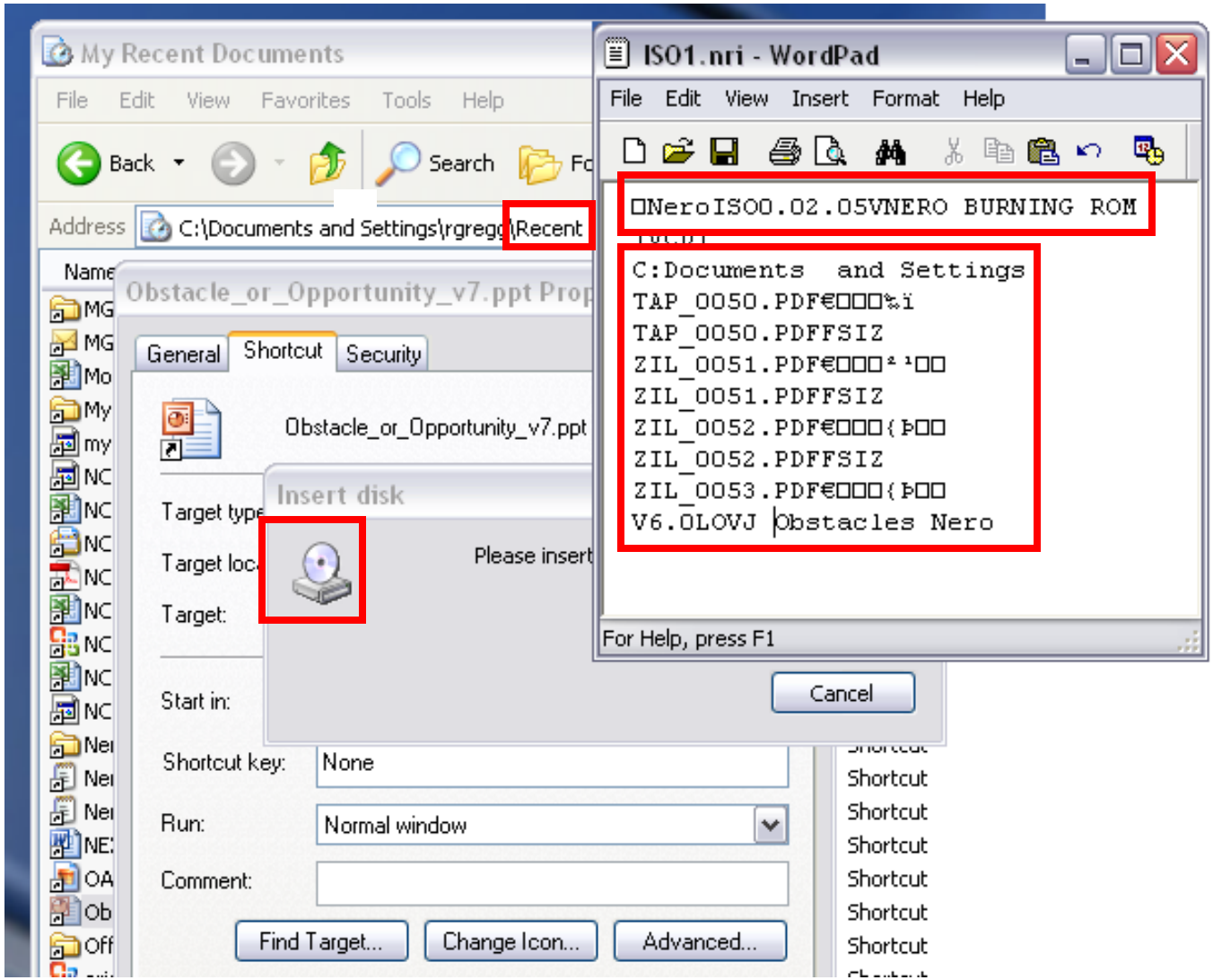
Web access (email, social media, cloud)

Travel

Data deletions

URL Name
http://www.google.com/search?source=ig&hl=en&rlz=&q=resignation letter examples&a
http://www.victorypharm
https://online.wellsfargo ession.cgi?sessargs
http://webmail.aol.com
http://www.facebook.com/login.php?email=jdoe@aol.com
file:///O:/Projects/2010/Wind Leases/Power Wind Lease2.doc
https://book.aircanada.com/pl/AConline/en/AC&FLIGHT=790 ODE=LAX
http://embassysuites US/es/hotel/MSPBRES es-Minneap
http://www.brothersoft. erase-deleted-files.html
http://www.google.com/search?source=ig&hl=en&rlz=&q=erasing deleted files&aq=0&o
http://bay102.mail.live.com/mail/InboxLight.aspx?Action=DeleteMessage&FolderID=000
javascript:onSubmitToolbarItemClicked('DeleteMessages','');

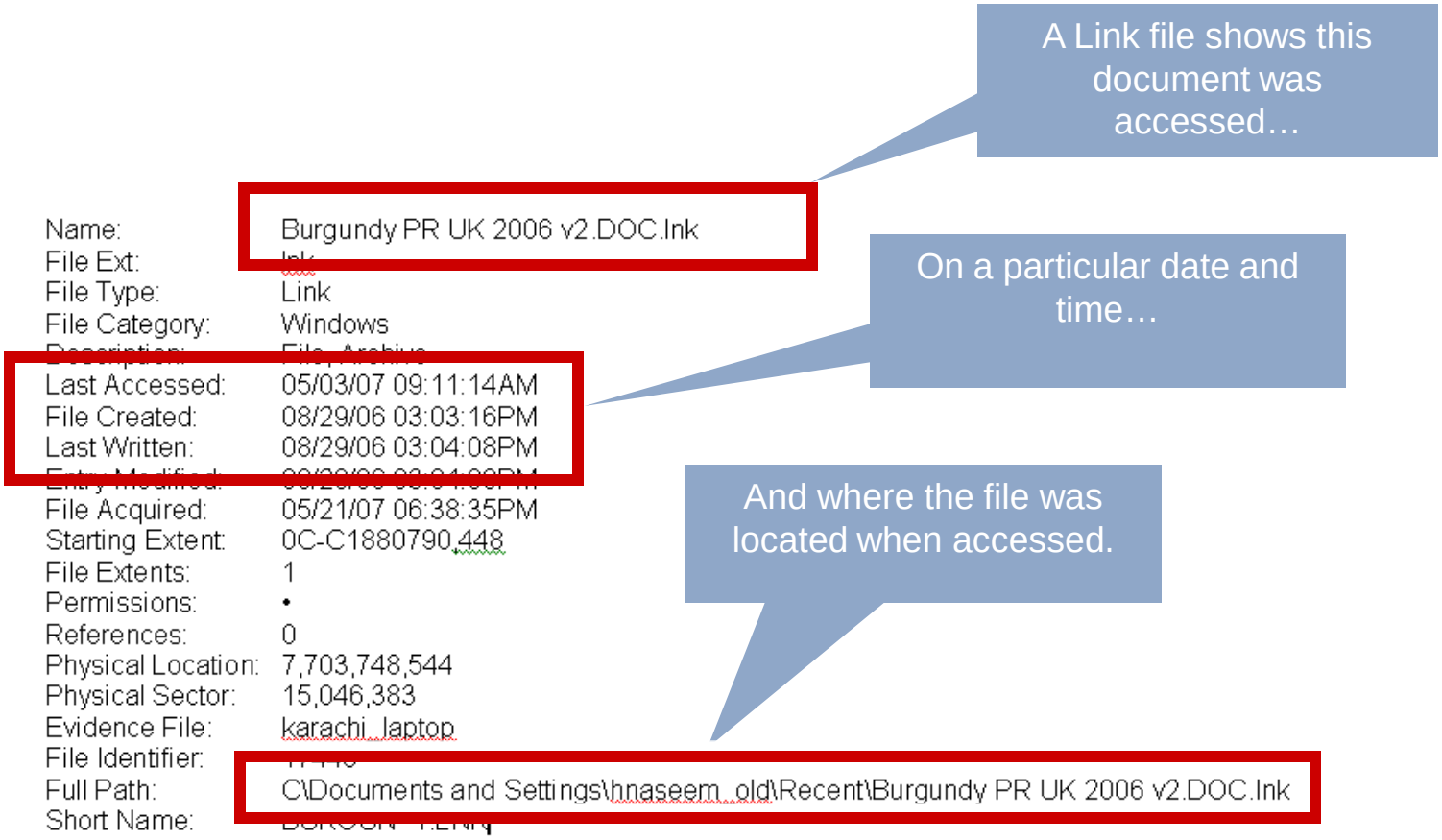
CD/DVD Burning



Removable Devices

- STORAGE
- SW
- UB1394
- USB
- USBPRINT
- USBSTOR
  - CdRom&Ven_SanDisk&Prod_U3_Titanium&Rev_2.18
  - Disk&Ven_Hitachi&Prod_HTS541260H9AT00&Rev_0811
  - Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_PMAP
  - Disk&Ven_RIM&Prod_BlackBerry_SD&Rev_0001
  - Disk&Ven_SanDisk&Prod_Cruzer_Micro&Rev_0.1
  - Disk&Ven_SanDisk&Prod_Cruzer_Mini&Rev_0.4
  - Disk&Ven_SanDisk&Prod_Cruzer_Titanium&Rev_2000
  - Disk&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_2.15
  - Disk&Ven_SanDisk&Prod_U3_Titanium&Rev_2.18
  - Disk&Ven_ST316081&Prod_5AS&Rev_
  - Disk&Ven_WDC_WD32&Prod_00BEVT-22ZCT0&Rev_
  - SFloppy&Ven_TEAC&Prod_FD-05PUB&Rev_1026
- V1394

Link File Analysis



Deletion and Wiping Activity

```
00000210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000250 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000260 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000270 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000280 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000290 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000002a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000002b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000002c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000002d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000002e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000002f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000300 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000310 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000320 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000330 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000340 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000350 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000360 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000370 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000380 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000390 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
```

SEARCH and ASSESS – External Threats

Spear Phishing

From: johnsmith985@yahoo.com

To: Joyce.associate@lawfirm.com

Subject: Please read the attachment for tomorrow's meeting.

Attachment: one document

Dear Joyce,

Please excuse the personal email address, I'm working from home and I can't get access to the network.

Can you please open the attached document and review for tomorrow's meeting.

Many thanks,

John

SEARCH and ASSESS – External Threat

- **Analyze log files.**
- **Review memory/virtual memory.**
- **Analyze hard drives.**
- **Analyze and reverse malware code.**
- **Review live traffic captures.**
- **Run behavioral profiling.**

Deleted Files: Hacker's Toolkit

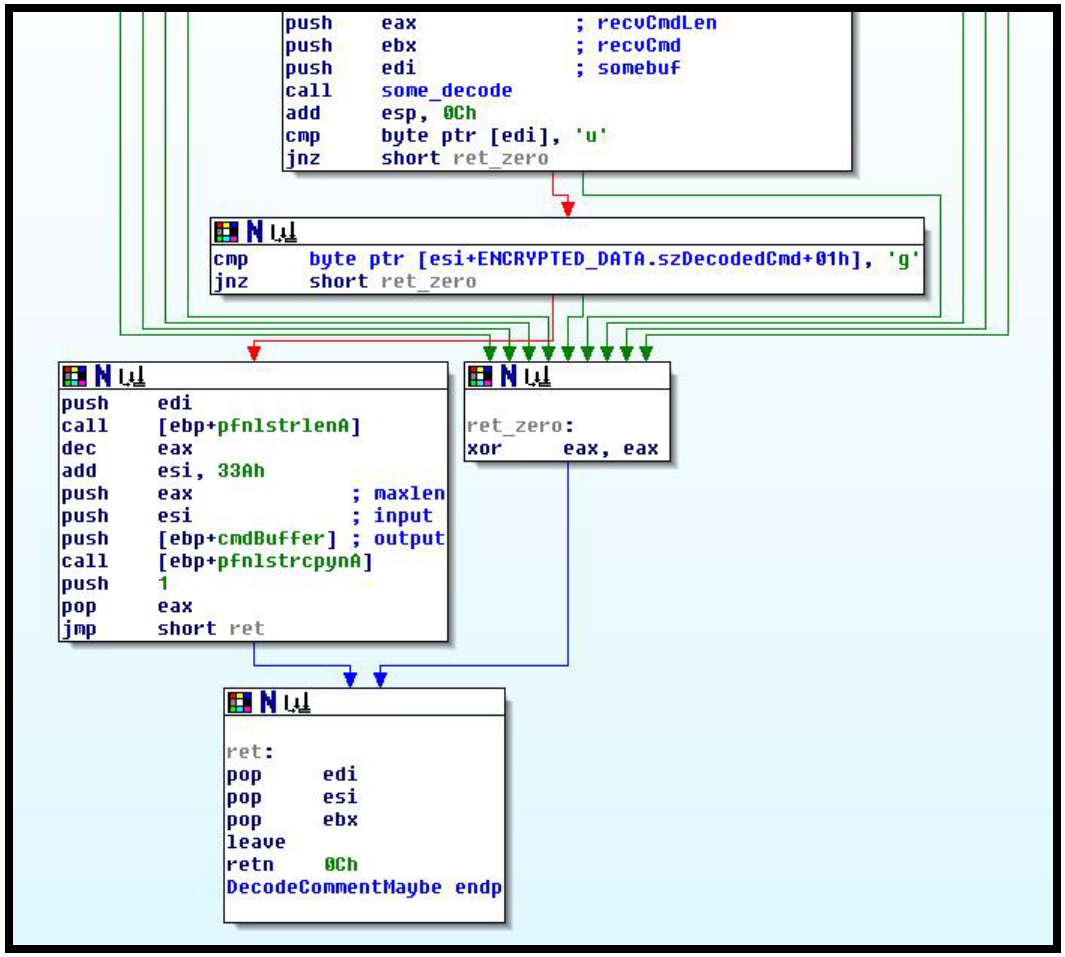
Name+	Type	Size
EraseLog.vbs+	VBScript Script File	1,109
FindPass.exe+	Application	17,408
Letmein.exe+	Application	18,432
ListAdmins.vbs+	VBScript Script File	1,213
Netsvc.exe+	Application	14,336
NETVIEWX.EXE+	Application	40,960
Psexec.exe+	Application	90,112
PsKill.exe+	Application	26,624
Psloggedon.exe+	Application	45,056
pspasswd.exe+	Application	57,344
Pulist.exe+	Application	55,296
rasmon.dll+	Application Extension	4,608
rasmon.exe+	Application	16,384
Sqlrcmd.asp+	ASP File	4,004

Volatile Data Capture

Capturing physical memory may reveal processes not normally seen by user or IT.

Proc#	PPID	PID	Name:
0	0	0	Idle
1	0	8	System
2	8	156	smss.exe
3	144	164	winlogon.exe
4	144	168	csrss.exe
5	156	176	winlogon.exe
6	156	176	winlogon.exe
7	156	180	csrss.exe
8	176	228	services.exe
9	176	240	lsass.exe
10	1112	284	dd.exe
11	820	324	helix.exe
12	228	408	svchost.exe
13	228	436	spoolsv.exe
14	228	464	Avsynmgr.exe
15	228	480	svchost.exe
16	228	540	regsvc.exe
17	228	552	MSTask.exe
18	228	592	dfrws2005.exe
19	464	612	VsStat.exe
20	464	628	Avconsol.exe
21	600	668	UMGR32.EXE
22	228	672	WinMgmt.exe
23	800	820	Explorer.Exe
24	820	964	Apoint.exe
25	820	972	HKserv.exe
26	820	972	HKserv.exe
27	820	988	DragDrop.exe
28	820	1008	alogserv.exe
29	820	1012	tgcmd.exe
30	820	1048	PcfMgr.exe
31	408	1064	JogServ2.exe
32	864	1072	Apntex.exe
33	820	1076	cmd.exe
34	592	1096	nc.exe
35	324	1112	cmd2k.exe

Malware Review



SEARCH and ASSESS – Challenges

Timing

- **Estimate per Server**
  - Initial Breach Analysis = 7 to 10 days
  - Identification of PII or PHI = 2 to 30 days
    (structured DB v. unstructured xls, doc, pdf, txt, jpg)

Desire for Certainty

- **Regulators**
- **Consumers**
- **Company Officers/Managers**

SEARCH and ASSESS – Challenges

Investigation Paradox

- **More careful analysis takes time**
- **More careful analysis increases certainty**
  - Can locate lost/stolen data
  - Can account for malware changes, attacking IP's
  - Can run scans across entire network
  - Can better account for PII and PHI sources
- **More careful analysis reduces cost**
- **2010 Ponemon Findings:**
  - Quick Responder* Cost = $268 per record

    Later Responder Cost = $174 per record

*notification within 30 days

SEARCH and ASSESS – Challenges

PII, PHI Variations:

- **Social security number:**

  === - == - ====, === == ====, ========,

  "SSN, Social Security Number, socsec," etc.

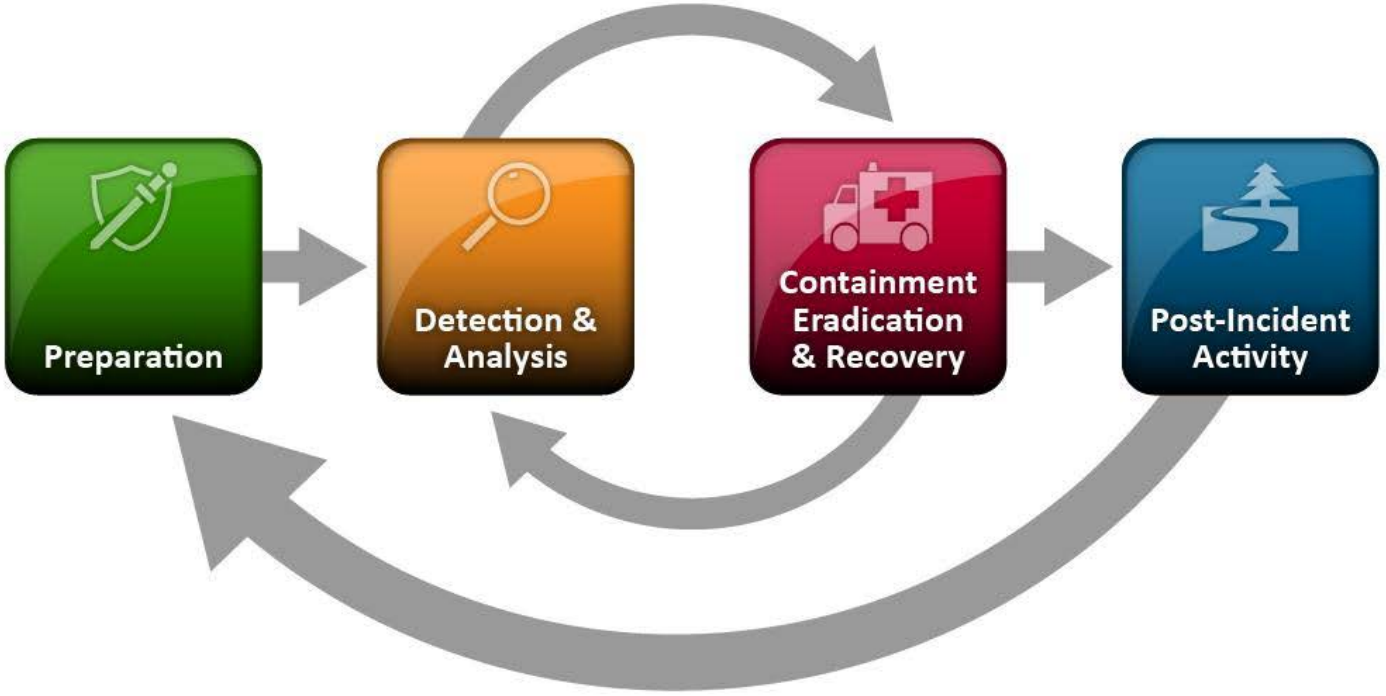
- **Account number:**

  5411222233334444 = 5.41122E+15 in scientific notation

- **Unsearchables:**

  SSN 000-00-1234
  SSN 000-00-5678

Breach Response – a Dynamic Process



Source: NIST - Computer Security Incident Handling Guide (Jan. 2012 Draft)

BREACH DEFINITIONS

Did an unauthorized party:

- **Access***
- **Acquire**
- **Misuse**
- **Disclose PII/PHI**

Does investigation show:

- **Material compromise**
- **Actual loss or injury to consumer**
- **Material risk of ID theft or fraud**
- **Significant risk of financial, reputational, other harm***

Internal Stakeholders

- Team Members –Counsel, Compliance, HR, IT, Business Managers, Public Affairs, Experts
- Board/CEO, Executives
- Employees
- Shareholders
- Customers

COMMUNICATE – Challenges

Notification Clock

- When did earliest/original breach occur?
- What is the notification due date?
- When will we “know” whether we need to notify?

Reporting Formats

- What are the needs of the response team?
- What does IT, Board, counsel need to know?
- Should reports be oral or written?
- What is covered by privilege?

Best Practices

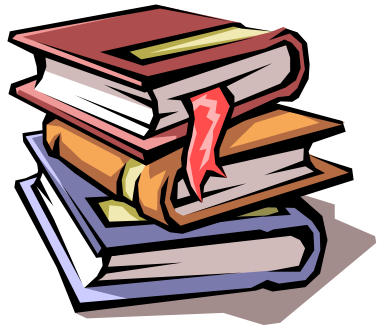
- Assemble response team immediately
- Discourage blame, data hoarding, and avoidance
- Communicate often, but not constantly
- Coordinate investigative findings across teams
- Limit strategic discussions to key managers & counsel

RESOURCES

HHS Health Information Privacy - ww.hhs.gov/ocr/privacy

NIST Computer Security Resource Ctr – csrc.nist.gov

State Data Breach Laws – www.ncsl.org



FTC Privacy Actions – www.ftc.gov/privacy

Privacy Rights – www.privacyrights.org

Open Security Foundation, Data Loss DB – datalossdb.org

QUESTIONS?

Paul H. Luehr
Managing Director, CPO
Stroz Friedberg

720 Northstar Center West
625 Marquette Ave South
Minneapolis, MN 55402

612.605-3007 direct
pluehr@strozfriedberg.com

Gerard M. Stegmaier, Esq.
Wilson Sonsini
Goodrich & Rosati, P.C.

1700 K Street, NW
Fifth Floor
Washington, DC 20006-3817

202-973-8809 direct
gstegmaier@wsgr.com