Legal Issues in Data Security
Ryan Kriger
Assistant Attorney General, Public Protection Division
October 20, 2016

Data Breaches:
Not Just Hackers
Data Incidents in 2015

What Kind Of Patterns Data Incidents Fall Into

Source: 2016 Verizon Data Investigations Report

Privilege Misuse

Any unapproved or malicious use of organizational resources . . . This is mainly insider-only misuse.

Frequency: 10,489 total incidents, 172 with confirmed data disclosure.

Source: 2016 Verizon Data Investigations Report
Data Incidents in 2015

Miscellaneous Errors
Incidents where unintentional actions directly compromised a security attribute of an information asset.
Frequency: 11,347 total incidents, 197 with confirmed data disclosure.

Protecting Sensitive Information

Traditional Confidential Information:
- Client Confidences & Secrets
- Information that Could Cause Embarrassment
- Attorney-Client Communications
- Work Product
- Confidential Document Productions (from Opposing Counsel)
- Trade Secrets

Source: 2016 Verizon Data Investigations Report
Protecting Sensitive Information

Statutorily Protected Information:
- Social Security Numbers
- Credit Card Numbers
- Financial Information
- Health Information
- Login Credentials

What do I mean by data breach

Unauthorized access to sensitive or confidential information:
- Losing consumer credit card numbers, SSNs, medical information, financial information
- Trade secret or otherwise confidential info produced by client or opposing counsel
- Work product or atty/client privileged info
How do Data Breaches happen?

- Hackers/Malware
- Phishing/Social Engineering/Lost Credentials
- Lost/Stolen Laptop, Smartphone, Thumb Drive
- Ex-Employee
- Accidental Disclosure (Production, Email, Posting to Internet)

How To Avoid Data Breaches
DATA SECURITY IS ABOUT

PEOPLE

What Can I Do To Avoid A Security Breach?

- Strong Passwords
- Email Hygiene
- Avoid Phishing/Pretexting
Strong Passwords

- Different Password for EVERY site
- Nonsense Characters & Numbers
- No Dictionary Words
- Change them occasionally

https://howsecureismypassword.net/

Strong Password Technique
amapacpciTi.05609

A Man A Plan A Canal
Panama
ciT (3rd char capitalized).
05609
Email Hygiene

- NEVER Be On Autopilot
- ALWAYS Be Skeptical
- NEVER Send Highly Sensitive Info via Email
- ALWAYS Pause Before
  - Clicking a Link
  - Opening an Attachment

So I Received An Email...

DO I KNOW THE SENDER? NO

DOES THE REQUEST SEEM REASONABLE? NO

IS THE EMAIL PERSONALIZED? NO

IS THERE A LINK OR ATTACHMENT? YES

IS THE EMAIL ASKING ME TO DO SOMETHING? (WIRE MONEY, SEND HIGHLY SENSITIVE DATA) YES

IGNORE?

PAUSE AND THINK BEFORE CLICKING

PICK UP THE PHONE AND CONFIRM
Highly Sensitive Info

- Social Security Numbers
- Bank Account or Financial Information
- Tax Return Information
- Health Information
- Passwords
- Anything Used for ID Theft

Alternatives to Regular Email

- Secure (Encrypted) Email Service
- Secure FTP
- (Internally) Shared File Server
- DVD/Thumb Drive/External HD (Encrypted)
- Paper
- NOT Cloud Drive
Scams to Avoid

- Phishing/Pretexting
  - CEO Scam
  - IRS/Bank Account Scam
- Lawyer Targeting Scam

Phishing

Out of 8 Million Results in Phishing Tests (2015)

- Median Time For 1st Open: 1 min, 40 sec
- Median Time for 1st Attachment Click: 3 min, 30 sec

Source: 2016 Verizon DBIR
Phishing Examples

Kriger, Ryan

From: "Concerned User"<email@email.com>
Sent: Wednesday, July 27, 2016 3:53 AM
Subject: ICT HelpDesk Upgrade

Your password will expire in 2 days. You will need to change your password, Click Here to continue

Best Regards
Technology Desk
IT-Service Team.

Phishing Examples

Kriger, Ryan

From: "Concerned User"<email@email.com>
Sent: Wednesday, July 27, 2016 3:53 AM
Subject: ICT HelpDesk Upgrade

View Dropbox from Cyrus: <email@email.com>

Hello,

Emailing files to people is a pain. Dropbox's shared folders let you share files with others, to view the documents, recipient, and other information, please click on the list below

Open file

When you save something to a shared folder, it'll be as if you saved it straight to your teammates' computer. When any changes are made, you'll see them instantly and get a notification tool.

Happy sharing!
- The Dropbox Team

Thank you for your login from the Dropbox server. If you have any questions about Dropbox, please call 1-800-671-0071

© 2016 Dropbox
Phishing Examples

From: [Redacted]

To: [Redacted]

Subject: RE: Dear Mailbox User

Dear Mailbox user,

Due to the current phishing attack on our mailing server, we have decided to migrate all staffs and students to the new 2016 outlook web server, which is going to protect you from receiving "phishing messages".

Kindly [click here] and sign in to migrate to the new 2016 outlook web server for safe and better mailing experience.

Note: Please do not fail to migrate to the new 2016 outlook web server as soon as this update gets to you because failure to migrate to the new 2016 outlook server, you won't be able to access your mailbox.

Contact the support centre for more information.

Connected to Microsoft Exchange,
© ADMIN TEAM 2016

I Got Breached, Now What?
Vermont’s Security Breach Notice Act

- 9 V.S.A. § 2430 and § 2435
- Applies to Businesses and State Agencies
  - Enforced by either AG or DFR (was BISHCA)
  - Does Not Apply to Certain Financial Institutions
- Applies to Loss of “Personally Identifiable Information”
- Amended Effective May 8, 2012

What is Personally Identifiable Information (PII)?

First Name or First Initial & Last Name (if it has not been encrypted or rendered unreadable), AND
- Social Security number; OR
- Motor vehicle operator’s license number or non-driver identification card number; OR
- Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; OR
- Account passwords or personal identification numbers or other access codes for a financial account.
Definition of “Security Breach”

“unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer’s personally identifiable information maintained by the data collector.”

Definition of “Security Breach”

“does not include good faith but unauthorized acquisition of personally identifiable information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information is not used for a purpose unrelated to the data collector’s business or subject to further unauthorized disclosure.”
Definition of “Security Breach”

Factors to consider when determining if a breach has occurred:

(i) Information is in someone else’s physical custody (i.e. stolen laptop);

(ii) Information has been downloaded or copied (i.e. hacking, malware, unauthorized use);

(iii) Information has been used by an unauthorized person (i.e. reports of fraudulent accounts opened or ID Theft); or

(iv) that the information has been made public.

I’ve Had a Data Breach, What Next?

1. Secure Your Data
2. Contact Law Enforcement
3. Contact Entities From Which You Obtained the Data
4. Notify the Attorney General’s Office Of The Breach
5. Notify Consumers Of The Breach
6. Notify the Credit Reporting Agencies (if more than 1,000 consumers)
Contact Law Enforcement

1. Call the FBI, Secret Service
2. Inform Them Of Your Duty To Notify Customers
3. Determine Whether Law Enforcement Wants You To Delay Notification

Timing of Notice Requirements

1. All Notices Should Go Out In The Most Expedient Time Possible
2. 14 Day Preliminary Notice to AG (non-public)
3. Final Notice to AG and to Customers (public) within 45 days
4. May only be delayed on request from law enforcement
## Contents of Notice Requirements

- Incident in general terms.
- Type of PII accessed
- General acts taken to protect the PII from further breaches
- Telephone number, toll-free if available, for further information.
- Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.
- The approximate date of the security breach.

## Manner of Notice Requirements

- **Direct Notice**
  - Mail
  - Email (if requirements are met)
  - Telephone (not prerecorded)
- **Substitute Notice (Website and Major Media)**
  - If cost would exceed $5,000
  - If number of customers exceeds 5,000
  - If insufficient contact information
No Harm Letter

- Notice Not Required if Misuse of Personal Information is Not Reasonably Possible
- Notice of this determination with detailed explanation sent to Vermont Attorney General

Penalty for Noncompliance

- Violation of the Consumer Protection Act
- $10,000 Civil Penalty per Violation
- Violation = Customer Not Noticed Per Day
A Tale of Two Data Breaches:

Two small VT businesses suffered a breach:
• One Acted Fast
• One Didn’t

What Happened?

How Should My Organization Protect Sensitive Data?
Have a Privacy and Data Security Plan:

- Who is responsible for protecting privacy?
- What data do you collect?
- Do you have a data breach plan?
- How do you destroy data?
- Do you have cyber insurance?

Have Data Collection Policies:

- Don’t collect data you don’t need
- Only keep data as long as you need it
- Consider using a 3rd party vendor to handle sensitive data
Basic Security Measures:

- Talk to Your IT People About Security
- Firewalls
- Anti-Virus Software
- Maintain Software Updates
- Change Default Passwords
- Authorization Control (who has access)?
- Beware products like LogMeIn (use a VPN)
- Home Computer Problems
- Physical Security
- Penetration Testing (Ask About Scan Vermont)

Watch Out For Portable Data:

- Cell Phones
- Tablets
- Laptops
- External Hard Drives
- Thumb Drives
- Data In Transit (including E-Mail)
- And Don’t Forget Back-up Tapes
Protect Portable Data:

- Password Protection
- Remote Wipe Capability
- Encryption
- Ask yourself: Should this be in a portable medium?

Encryption:

- Encrypt mobile media
- Encrypt data in transit
- Don’t store encryption keys with your encrypted data
- Consider encrypting backups
Questions About Data Breaches?

- Call Us
- 802-828-3171
- ago.datasecurity@vermont.gov

Vermont Bar Assoc. Advisory Ethics Opinion 2010-6

Addresses:
- The propriety of attorneys and firms using Software as a Service ("SaaS"), aka Cloud Computing.
- Whether client docs and info can be remotely stored and backed up in the Cloud.
- Whether lawyers can use cloud/web-based email and calendar systems.
- Whether use of remote doc synchronization systems is permissible.
Vermont Bar Assoc. Advisory Ethics Opinion 2010-6

Conclusion:

• Due to rapidly changing technology, not appropriate to establish a checklist of specific conditions precedent factors
• Lawyer should undertake reasonable due diligence of cloud vendor

Factors that should “often” be taken into account:

• the vendor’s security system;
• what practical and foreseeable limits, if any, may exist to the lawyer’s ability to ensure access to, protection of, and retrieval of the data;
• the material terms of the user agreement;
• the vendor’s commitment to protecting confidentially of the data;
• the nature and sensitivity of the stored information;
• notice provisions if a third party seeks or gains (whether inadvertently or otherwise) access to the data; and
• other regulatory, compliance, and document retention obligations that may apply based upon the nature of the stored data and the lawyer’s practice.
Vermont Bar Assoc. Advisory Ethics Opinion 2010-6

The lawyer should consider:

- giving notice to the client about the proposed method for storing client data;
- having the vendor’s security and access systems reviewed by competent technical personnel;
- establishing a system for periodic review of the vendor’s system to be sure the system remains current with evolving technology and legal requirements; and
- taking reasonable measures to stay apprised of current developments regarding SaaS systems and the benefits and risks they present.

Vermont Bar Assoc. Advisory Ethics Opinion 2010-6

Other Conclusions:

- Use of Cloud/SaaS generally ok, if reasonable precautions taken to make sure property:
  - Secure
  - Accessible
- Nature of Precautions depends on circumstances
- Location of remote server not a limiting factor, but:
  - Consider Choice of Law clauses
  - Consider access to data
- Some client property should not be stored on remote servers (case specific analysis)
  - Original wills
  - Docs subject to permanent retention obligations
  - Trade secrets may not be appropriate for storage based on security
- Use of cloud for email, calendar, remote synchronization, similar issues
Concerns About Technology Generally

Precautions lawyers should take:

- Provide adequate physical protection for devices (e.g., laptops)
- Have methods for deleting data remotely in the event that a device is lost or stolen
- Use strong passwords
- Purge data from devices before they are replaced (e.g., computers, smart phones, and copiers with scanners)
- Install appropriate safeguards against malware (e.g., virus & spyware protection)
- Install adequate firewalls to prevent unauthorized access to locally stored data
- Ensure frequent backups of data
- Update operating systems to ensure that they contain the latest security protections
- Configure software and network settings to minimize security risks
- Encrypt sensitive information, and identify (and, when appropriate, eliminating) metadata from electronic documents before sending them
- Avoid “wifi hotspots” in public places as a means of transmitting confidential information (e.g., sending an email to a client)

Cal Bar Opinion No. 2010-179
(Use of Technology to Store and Transmit Confidential Info)

Factors to consider when using a new technology:

- Attorneys ability to assess the level of security afforded:
  - how it differs from other media
  - whether reasonable precautions may be taken
  - limitations on ability to monitor technology
- Legal ramifications of 3rd-Parties intercepting/accessing info
- Degree of sensitivity of the information
- Possible Impact on the client of inadvertent disclosure (including possible waiver of privileges)
- Urgency of the situation
- Client instructions and circumstances

Source: Sept. 20, 2010 ABA Issues Paper Concerning Client Confidentiality and Lawyers Use of Technology

Factors to consider when using a new technology:
Cal Bar Opinion No. 2010-179
(Use of Technology to Store and Transmit Confidential Info)

Conclusions:
• It’s not OK to use a coffee shop wireless connection to work on a client’s confidential matter unless takes precautions:
  ◦ File encryption
  ◦ Encryption of wireless transmissions
  ◦ Personal Firewall
• For highly sensitive info it may never be ok to use a public wireless connection
• It’s OK to use a home wifi connection if it has appropriate security

Social Security Number Protection Act

• 9 V.S.A. §§ 2440, 2445
• Applies to businesses and state agencies
• Businesses must safely destroy records that Contain Social Security Numbers and other personal information
Social Security Number Protection Act

A business may not:

- Make SSN’s Public
- Put a SSN on a membership card
- Require non-secure or non-encrypted internet transmission of SSN’s
- Require SSN to logon to website, unless with password or PIN
- Print SSN on mailings (unless required by law)
- Disclose SSNs to 3rd Parties without Written Consent

Social Security Number Protection Act

Exceptions:

- SSN mailed in application or account documents, but not on a postcard or on the envelope
- Use of SSN “reasonably necessary for administrative purposes or internal verification”
- Opening of account or the provision of or payment for a product or service authorized by an individual
- Acting pursuant to a court order, subpoena, otherwise required by law
- Providing SSNs to government entity, including law enforcement
- Redacted SSN
- Info obtained from official records or court records
- Use by business prior to 1/1/2007
Social Security Number Protection Act

Exceptions – Use of SSN to:
- investigate or prevent fraud
- conduct background checks
- conduct social or scientific research
- collect a debt
- obtain a credit report from or furnish data to a consumer reporting agency pursuant to the fair credit reporting act
- undertake a permissible purpose enumerated under Gramm Leach Bliley
- locate an individual who is missing, is a lost relative, or is due a benefit, such as a pension, insurance, or unclaimed property benefit.

Unfair and Deceptive Acts Statutes

- Vermont’s Consumer Protection Act
- The FTC Act
- Prohibits Unfair and Deceptive Acts
- Unfair: Collecting Sensitive Information and Failing to Properly Protect It
- Deceptive: Advertising That You Protect Information When You Do Not
HIPAA
- Health Insurance Portability and Accountability Act
- Applies to Health Plans, Health Care Providers and Health Care Clearinghouses
- Protection of Personal Health Information
- Privacy Rule and Security Rule

COPPA
- Children's Online Privacy Protection Act
- Applies to Website Operators that collect personal information from children under 13
- Requires Privacy Notice & Verifiable Parental Consent for Collection, Use and Disclosure of Personal Information
- Privacy Rule and Security Rule
- http://www.coppa.org
Gramm-Leach-Bliley Act

- Applies to Financial Institutions (companies that offer consumers financial products or services like loans, financial or investment advice, or insurance)
- Requires Companies that offer financial services to give consumers privacy notices that explain their information-sharing practices

DFR (formerly BISHCA) Regs

- Regulation B-2001-01: Governs treatment of nonpublic personal info about consumers by financial institutions
- Regulation IH-2001-01: Governs treatment of nonpublic personal financial and health info about consumers by licensees under 8 V.S.A. Parts 3 & 4
- Regulation IH-2002-03: Standards for protecting security, confidentiality, and security of customer info under Gramm-Leach-Bliley
Online Resources

- OnGuardOnline.gov
- business.ftc.gov
- IAPP: www.privacyassociation.org
The U.S. Federal Bureau of Investigation (FBI) this week warned about a “dramatic” increase in so-called “CEO fraud,” e-mail scams in which the attacker spoofs a message from the boss and tricks someone at the organization into wiring funds to the fraudsters. The FBI estimates these scams have cost organizations more than $2.3 billion in losses over the past three years.

In an alert posted to its site, the FBI said that since January 2015, the agency has seen a 270 percent increase in identified victims and exposed losses from CEO scams. The alert noted that law enforcement globally has received complaints from victims in every U.S. state, and in at least 79 countries.

CEO fraud usually begins with the thieves either phishing an executive and gaining access to that individual’s inbox, or emailing employees from a look-alike domain name that is one or two letters off from the target company’s true domain name. For example, if the target company’s domain was "example.com," the thieves might register "examp1e.com" (substituting the letter "L" for the numeral 1) or "example.co," and send messages from that domain.

Unlike traditional phishing scams, spoofed emails used in CEO fraud schemes rarely set off spam traps because these are targeted phishing scams that are not mass e-mailed. Also, the crooks behind them take the time to understand the target organization’s relationships, activities, interests and travel and/or purchasing plans.

They do this by scraping employee email addresses and other information from the target’s Web site to help make the missives more convincing. In the case where executives or employees have their inboxes compromised by the thieves, the crooks will scour the victim’s email correspondence for certain words that might reveal whether the company routinely deals with wire transfers — searching for messages with key words like "invoice," “deposit” and “president.”

On the surface, business email compromise scams may seem unsophisticated relative to moneymaking schemes that involve complex malicious software, such as Dyre and ZeuS. But in many ways, CEO fraud is more versatile and adept at sidestepping basic security strategies used by banks and their customers to minimize risks associated with account takeovers. In traditional phishing scams, the attackers interact with the victim’s bank directly, but in
the CEO scam the crooks trick the victim into doing that for them.

The FBI estimates that organizations victimized by CEO fraud attacks lose on average between $25,000 and $75,000. But some CEO fraud incidents over the past year have cost victim companies millions — if not tens of millions — of dollars.

Last month, the Associated Press wrote that toy maker Mattel lost $3 million in 2015 thanks to a CEO fraud phishing scam. In 2015, tech firm Ubiquiti disclosed in a quarterly financial report that it suffered a whopping $46.7 million hit because of a CEO fraud scam. In February 2015, email con artists made off with $17.2 million from The Scoular Co., an employee-owned commodities trader. More recently, I wrote about a slightly more complex CEO fraud scheme that incorporated a phony phone call from a phisher posing as an accountant at KPMG.

The FBI urges businesses to adopt two-step or two-factor authentication for email, where available, and to establish other communication channels — such as telephone calls — to verify significant transactions. Businesses are also advised to exercise restraint when publishing information about employee activities on their Web sites or through social media, as attackers perpetrating these schemes often will try to discover information about when executives at the targeted organization will be traveling or otherwise out of the office.

For an example of what some of these CEO fraud scams look like, check out this post from security education and awareness firm Phishme about scam artists trying to target the company’s leadership.

I’m always amazed when I hear security professionals I know and respect make comments suggesting that phishing and spam are solved problems. The right mix of blacklisting and email validation regimes like DKIM and SPF can block the vast majority of this junk, these experts argue.

But CEO fraud attacks succeed because they rely almost entirely on tricking employees into ignoring or sidestepping some very basic security precautions. Educating employees so that they are less likely to fall for these scams won’t block all social engineering attacks, but it should help. Remember, the attackers are constantly testing users’ security awareness. Organizations might as well be doing the same, using periodic tests to identify problematic users and to place additional security controls on those individuals.

Tags: ceo fraud, dkim, Dyre, fbi, phishme, spf, The Scoular Co., Ubiquiti, zeus

This entry was posted on Thursday, April 7th, 2016 at 10:36 am and is filed under A Little Sunshine, Latest Warnings, The Coming Storm. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.
Counterfeit check scams continue to target law firms

A lawyer receives what appears to be a legitimate solicitation email from a prospective client seeking representation in a debt collection matter. The terms of a relationship, including a fee agreement, may be negotiated. The lawyer then receives what appears to be a valid cashier's check, supposedly a settlement check from a debtor, from a reputable bank. After the money is deposited in the lawyer's client trust account, the "client" asks that the funds, less the fees, be wired to a foreign bank.

The cashier's check was fraudulent and the lawyer is left holding the bag.

This scenario continues to be replayed as part of a sophisticated Internet scam that often targets collection lawyers. The Santa Clara District Attorney's office recently was alerted by a local law firm that was contacted by a "client" who said his east coast company provided materials to a local medical company that hadn't paid its bill. The out-of-state company provided legitimate-looking documents, such as contracts and invoices, to support its claim, and the law firm found a website for the client's company. A retainer agreement was executed.

The client said it would make a last ditch attempt to collect the debt before authorizing a lawsuit. Two days later, the firm received a $270,000 cashier's check from the medical company. The client told the firm to withhold its fee, plus a little extra, and wire the remaining funds to an account that turned out to be overseas. Despite pressure from the client for the money, the law firm waited for the check to clear.

That never happened.

The alleged debtor was a real company that was not involved with the "client," who remains unidentified and may be located overseas. According to Santa Clara County Deputy district Attorney Mike Fletcher, the suspects "generated very authentic-looking documents, created a website and are executing a sophisticated scheme with the potential to significantly harm law firms."

But in addition to winding up with an overdrawn bank account, victims can face State Bar discipline and damage to his or her reputation. In order to help lawyers avoid being taken in, the bar's Committee on Professional Responsibility and Conduct (COPRAC) issued an ethics alert earlier this year describing both how the scams work and how lawyers can protect themselves.

The scam leaves the lawyer appearing to have retained a client, triggering various ethical duties governed by professional responsibility rules. The ethics alert offers both a warning and suggestions for how lawyers can protect themselves.

"If it is too good to be true, it usually is," the alert concludes. "Hitting the delete button may be the best course of action for the attorney, not to mention those caught up in the cascade of adverse consequences of a successful scam."

The FBI reports the debt collection scam is well-known and occurs nationwide. Another scheme has the fraudulent client posing as an ex-wife "on assignment" in an Asian country and pursuing collection of divorce settlement funds from her ex-husband in the U.S. Once a law firm agrees to represent the wife and contacts the ex-husband, it receives a "certified" settlement check. As with other scams, the wife instructs the firm to wire the funds, less its retainer fee, to an overseas bank account.

If funds are sent before discovering the check is counterfeit, the firm is left in the lurch.

The FBI urges firms or victims of an internet scam to file a complaint with the Internet Crime Complaint Center.
Counterfeit check scams continue to target law firms