



# Stealth Attacks and Cyber Security

Dauphin County Bar Association

March 10, 2020

Robert Davis, Esq  
Mark LeFever, USI Affinity  
Gina Sage, USI Affinity

1

**DAUPHIN COUNTY BAR – MARCH 10, 2020**  
**Narrative of Cyber Stealth Attack and FCS and Ethics Complaint \*\*\***



The Davis Firm had a long and successful history of serving as the settlement agent for Real Estate transfers. In November the Davis Firm office acted as settlement agent for a transfer between a buyer, Abel and the Seller, Sam. Prior to settlement the Davis Firm real estate paralegal, an experienced paralegal with many years of successful and error-free work, received an email from a sender whose name and email address appeared as identical to the Seller Sam, confirming the time for settlement later that day. There had been email contacts with Seller Sam prior to that time. At the conclusion of settlement on November 18th, Davis Firm gave Seller Sam a check for their proceeds in the amount of \$70,000.00. Shortly after settlement the real estate paralegal received an email from the same email address as had made the morning contact re scheduling, indicating that Seller Sam had changed his mind and needed the proceeds to be wired into their account. Our real estate paralegal instructed them that she cannot wire the proceeds without first having the physical check that was provided to the seller at settlement, returned to the Davis office. The sender of the emails indicated that the check had been shredded and they could not bring it back to the Davis Firm. The email sender provided wire instructions for a bank account in New York which included the name of the actual seller from that day's settlement. Specifically, the name given for the account was "Sam Seller, Inc.". The culmination of this interaction was that the real estate paralegal wired \$70,000.00 to the account for which she was given instructions by the person who claimed to be Seller Sam through the email.

2



On November 19th the actual sellers deposited their check into their bank account. That day the wire also was withdrawn from the Davis Firm escrow account. Due to the intervening Thanksgiving Holiday the Davis Firm office was closed on November 22 and 23. On November 26, the Davis Firm office reopened and our real estate paralegal received a call from our Bank, Best Community Bank (“BCB”), indicating that there was an overdraft of the Davis real estate (IOLTA) account. It was at this time that our real estate paralegal reviewed our escrow account and discovered the theft. To prevent further fees from being charged against our account for overdraft and to prevent other client related checks from being returned for insufficient funds, we immediately deposited \$70,000 from our Office Operating Account into our real estate escrow (IOLTA) account. We believe that this action was necessary to protect our clients and our IOLTA account. We understood that our funds will likely never be recovered but we saw no good alternative to protect our clients’ interests.

On November 26 or 27 after this theft was discovered by our staff, we immediately filed a report with the Pennsylvania State Police (Jonestown Barracks) as well as BCB from which money was wired. The Pennsylvania State Police are continuing to investigate this matter. We have received notification from the State Police that the money that was wired was immediately withdrawn from the account in New York. The Police also indicated that the account in New York was also the recipient of other fraudulent wires from other settlement companies. Our bank has made requests to both the bank that received the wire as well as the FED line service which banks use in such situations, to attempt to recover the funds that were taken.

On about November 26 or 27 the Davis Firm also contacted its insurance agency (CNA) and explained what had happened. We were told that our existing policy does not cover this type of cyber fraud or theft.

3



On approximately November 30 the Davis Firm received a letter from the Pennsylvania Lawyers Fund for Client Security dated November 29, a standard procedure when a check on an IOLTA is dishonored. This letter directed us to provide bank statements along with a written explanation for the overdraft of our IOLTA account.

On December 13 the Davis Firm received a second letter from the Lawyers Fund for Client Security acknowledging receipt of our letter and indicating that the matter was sent to the Office of Disciplinary Counsel [ODC] for its investigation, a standard referral. We were required to again give a detailed explanation to the ODC. The Davis Firm reported the incident to CNA as the matter was now an ethics/licensing claim. It reported the detail of the scam and provided the emails and all financial accounts to the ODC, including proof that the firm had acted promptly to protect its clients and had, in effect lost \$70,000 of its own money as a result of the scam. The Davis Firm expected a dismissal as its staff was well-trained and had been fooled by a very slick scam in which the thieves had somehow learned the name and time of the closing somehow in order to insert its false email address into Davis Firm records and had fooled an otherwise very competent, experienced paralegal into sending the wire transfer of funds.

The ODC added insult to injury by closing the complaint by summary disposition – issuing a “Letter of Education” which stated that the managing attorneys “could have done more to assure that settlement funds went to the right party.” They were also critical that the Davis Firm had allowed the experienced paralegal to handle the settlement, saying that in their (totally inexperienced in the real world view) opinion, the paralegal had not been supervised closely enough.

4



Since this incident the Davis Firm has taken several steps to prevent any future occurrence of this kind but is wondering if this is enough to avoid the type of skillful theft it had suffered:

- The Firm had its IT professional (they have one, another proof of competence/care) scan all of the office computers and server for virus and / or malware. He found that there was no virus or malware on our computers or servers;
- The IP address of the computer from which the Davis Firm real estate paralegal works was changed;
- The Davis Firm closed the net teller account at BCB bank which was used for its real estate account and opened a new ID;
- The Firm instituted a policy that one of the Attorneys at the office must always sign to approve any future outgoing wire;
- The Firm created and instituted a two-step verification process (including password and personal information) that must be undertaken before the type of settlement proceeds can ever be changed by a seller before or after a real estate settlement;
- The Davis Firm also took information and advice provided by both the PA State Police and our bank's security team to do an employee training in recognizing this type of attempted fraud.

\*\*\* This is taken from the actual client narrative provided to defend the ethics complaint

5

5



### Accused ringleader in scam that bilked \$70M from law firms has taken plea

A foreign citizen accused of acting as a ringleader in a scheme in which prosecutors say U.S. and Canadian law firms were scammed out of some \$70 million has pleaded guilty in federal court in Harrisburg, Pa.

Emmanuel Ekhaton, 42, pleaded guilty earlier this year to conspiracy to commit mail fraud and wire fraud, admitting responsibility for up to \$20 million in law firm losses. A resident of Mississauga, Canada, and Benin City, Nigeria, who was seeking refugee status in Canada, he had been living in Toronto while coordinating the fraud ring, reports the Toronto Star.

The scheme involved a group of individuals who initially contacted law firms by email, routinely claiming to be foreign residents seeking representation to collect money owed them by a U.S. entity, often from a tort claim settlement, divorce or real estate transaction. After the firm agreed to the representation, the purported third party would then contact the firm and offer to send a cashier's check in settlement of the claim. The firm would deposit the bank check in its trust account, wire the settlement proceeds to the foreign "client" and retain the agreed fee before discovering that the check was a fake, explains a press release from the U.S. Attorney's Office for the Middle District of Pennsylvania.

6

6



(continued)

Lawyers who have discussed being victimized in such schemes have said banks involved in cashing the check verified that it was good and cleared the funds, but later notified the firm that the check was a fake and sought reimbursement.

The press release says counterfeit checks "often included a telephone number for the financial institution. Lawyers attempting to determine the validity of the check would call the number only to reach another conspirator who would falsely verify the check."

Barbara Nevin of Milavetz, Gallop & Milavetz confirmed that her Minneapolis area firm suffered such a loss in 2009 but declined to discuss the fraud in detail prior to Ekhatov's sentencing.

"It was a very sophisticated scam," she told the Star, explaining "You have someone purporting to be a client and they have other people that are in this with them pretending to be insurance adjusters."

Ekhatov faces up to 20 years when he is sentenced in June and he has agreed to forfeit property in Canada and bank accounts in Nigeria.



**Phishing Attacks**

When you think of "cyber-attacks," what comes to mind? If you're like a lot of people, you imagine hackers launching complex attacks against international corporations and governments. The reality is that one of the most common types of cyber-attacks are phishing attacks. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computer with viruses or malware, creating vulnerability to attacks. Phishing emails may **appear** to come from a legitimate financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information like account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access their accounts.

**Phishing attacks:** are incredibly easy to do – hackers don't need high-tech skills and tools; target human beings instead of machines, which are easier to trick; target a high number of people to increase the likelihood of success with minimum effort. This is why these attacks are so dangerous and are on the rise - impacting lots of American businesses.


**Phishing Examples**

The following messages, from the Federal Trade Commission's OnGuardOnline (<https://www.consumer.ftc.gov/features/feature-0038-onguardonline>), are examples of what attackers may email or text when phishing for sensitive information:

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."



**Simple Safety Tips**

**When in doubt, throw it out:** Links in email and online posts are often the way cybercriminals compromise your computer. If it looks suspicious – even if you know the source – it’s best to delete or, if appropriate, mark it as “junk email.” Contact the sender directly (via phone) to be sure the email is legitimate.

**Think before you act:** Be wary of communications that request for you to act immediately, offer something that sounds too good to be true, or ask for personal information.

**Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.

**Install and update anti-virus software:** Make sure all of your computers are equipped with regularly updated antivirus software, firewalls, email filters, and antispyware.

**Be wary of hyperlinks:** Avoid clicking on hyperlinks in emails; type the URL directly into the address bar instead. If you choose to click on a link, ensure it is authentic before clicking on it. You can check a hyperlinked word or URL by hovering the cursor over it to reveal the full address.

**Four eye-opening facts about phishing**


The Webroot Phishing Threat Trends report ([https://webroot-cms-cdn.s3.amazonaws.com/7314/8070/2914/Webroot\\_Threat\\_Trends\\_December\\_2016.pdf](https://webroot-cms-cdn.s3.amazonaws.com/7314/8070/2914/Webroot_Threat_Trends_December_2016.pdf)) identified four eye-opening facts about phishing that all companies should be aware of:

**The lifecycle of a phishing site is, on average, under 15 hours** - The lifecycle of phishing sites has now shrunk to an average of 15 hours, spanning from 15 minutes through to 44 hours.

**Almost all phishing URLs are hidden within benign domains** - Phishing attacks don’t use new dedicated domain names anymore because they can be easily identified and blacklisted. Almost all phishing attacks now “use domains typically associated with benign activity” to increase the probability of their success. Hackers prefer to compromise a single page of a benign site and replace its content with a phishing page, which is more difficult to detect.

9

9



**An average of over 400,000 phishing sites have been observed each month this year** - hackers are forced to increase the number of phishing sites since the lifecycle doesn’t last long.

**The most impersonated companies are google, yahoo, apple, PayPal/Wells Fargo** – “Impersonating world-renowned tech companies seems to be the trend. Of all phishing sites detected between January and October 2016, Google was the most-impersonated brand (21%), followed by Yahoo (19%), Apple (15%), PayPal and Wells Fargo (both 13%).”

**To avoid falling victim to phishing attacks, use your brain...**

There is no tech defense against phishing attacks that guarantees security because it’s up to a human who decides to click the malicious link. The more that people are aware of phishing and its risks, the less likely they are going to fall for a phishing attack – and avoid putting the whole company at risk.

*References*

1. <https://www.dhs.gov/sites/default/files/publications/Phishing%20508%20compliant%20508%20compliant.pdf>
2. <https://inspiredelearning.com/resource/phishing-statistics-threat-business/>
3. <https://www.itgovernance.co.uk/blog/4-eye-opening-facts-about-phishing/>

10

10



## How do you know if your privacy is being protected?

**Privacy policy** - Before submitting your name, email address, or other personal information on a website, look for the site's privacy policy. This policy should state how the information will be used and whether or not the information will be distributed to other organizations. Companies sometimes share information with partner vendors who offer related products or may offer options to subscribe to particular mailing lists. Look for indications that you are being added to mailing lists by default—failing to deselect those options may lead to unwanted spam. If you cannot find a privacy policy on a website, consider contacting the company to inquire about the policy before you submit personal information, or find an alternate site. Privacy policies sometimes change, so you may want to review them periodically.

### What additional steps can you take to protect your privacy?

**Do business with credible companies** - Before supplying any information online, consider the answers to the following questions: do you trust the business? is it an established organization with a credible reputation? does the information on the site suggest that there is a concern for the privacy of user information? is there legitimate contact information provided? Check online companies history at <http://www.resellerratings.com> or a similar service.

**Do not use your primary email address in online submissions** - Submitting your email address could result in spam. If you do not want your primary email account flooded with unwanted messages, consider opening an additional email account for use online. Make sure to log in to the account on a regular basis in case the vendor sends information about changes to policies.




**Avoid submitting credit card information online** - Some companies offer a phone number you can use to provide your credit card information. Although this does not guarantee that the information will not be compromised, it eliminates the possibility that attackers will be able to hijack it during the submission process.

**Devote one credit card to online purchases** - To minimize the potential damage of an attacker gaining access to your credit card information, consider opening a credit card account for use only online. Keep a minimum credit line on the account to limit the amount of charges an attacker can accumulate.

**Avoid using debit cards for online purchases** - Credit cards usually offer some protection against identity theft and may limit the monetary amount you will be responsible for paying. Debit cards, however, do not offer that protection. Because the charges are immediately deducted from your account, an attacker who obtains your account information may empty your bank account before you even realize it.

**Take advantage of options to limit exposure of private information** - Default options on certain websites may be chosen for convenience, not for security. For example, avoid allowing a website to remember your password. If your password is stored, your profile and any account information you have provided on that site is readily available if an attacker gains access to your computer. Also, evaluate your settings on websites used for social networking. The nature of those sites is to share information, but you can restrict access to certain information so that you limit who can see what.




**Evidence that your information is being encrypted** - To protect attackers from hijacking your information, any personal information submitted online should be encrypted so that it can only be read by the appropriate recipient. Many sites use SSL, or secure sockets layer, to encrypt information. Indications that your information will be encrypted include a URL that begins with "https:" instead of "http:" and a lock icon in the bottom right corner of the window. Some sites also indicate whether the data is encrypted when it is stored. If data is encrypted in transit but stored insecurely, an attacker who is able to break into the vendor's system could access your personal information.

Mindi McDowell. *Protecting Your Privacy*, <http://www.us-cert.gov/cas/tips/ST04-013.html>

13

13



## Defending Cell Phones and PDAs Against Attack

As cell phones and PDAs become more technologically advanced, attackers are finding new ways to target victims. By using text messaging or email, an attacker could lure you to a malicious site or convince you to install malicious code on your portable device.

**What unique risks do cell phones and PDAs present?**

Most current cell phones have the ability to send and receive text messages. Many cell phones and PDAs also offer the ability to connect to the internet. Although these are features that you might find useful and convenient, attackers may try to take advantage of them. As a result, an attacker may be able to accomplish the following:

**abuse your service** - Most cell phone plans limit the number of text messages you can send and receive. If an attacker spams you with text messages, you may be charged additional fees. An attacker may also be able to infect your phone or PDA with malicious code that will allow them to use your service. Because the contract is in your name, you will be responsible for the charges.

**lure you to a malicious web site** - While PDAs and cell phones that give you access to email are targets for standard phishing attacks, attackers are now sending text messages to cell phones. These messages, supposedly from a legitimate company, may try to convince you to visit a malicious site by claiming that there is a problem with your account or stating that you have been subscribed to a service. Once you visit the site, you may be lured into providing personal information or downloading a malicious file.

**use your cell phone or PDA in an attack** - Attackers who can gain control of your service may use your cell phone or PDA to attack others. Not only does this hide the real attacker's identity, it allows the attacker to increase the number of targets.

**gain access to account information** - In some areas, cell phones are becoming capable of performing certain transactions (from paying for parking or groceries to conducting larger financial transactions). An attacker who can gain access to a phone that is used for these types of transactions may be able to discover your account information and use or sell it.

14

14



**What can you do to protect yourself?**

**Follow general guidelines for protecting portable devices** - Take precautions to secure your cell phone and PDA the same way you secure your computer. Make sure your portable device has a secure password.

**Be careful about posting your cell phone number and email address** - Attackers often use software that browses web sites for email addresses. These addresses then become targets for attacks and spam. Cell phone numbers can be collected automatically, too. By limiting the number of people who have access to your information, you limit your risk of becoming a victim.

**Do not follow links sent in email or text messages** - Be suspicious of URLs sent in unsolicited email or text messages. While the links may appear to be legitimate, they may actually direct you to a malicious web site. Don't respond to text messages from people you do not know.

**Be wary of texting for contests or virtual voting** - These seeming "free" and "fun" activities are often ways to gain access to your cell phone # to be used for future promotions, advertising and sometimes malicious activity.

**Be wary of downloadable software** - There are many sites that offer games and other software you can download onto your cell phone or PDA. This software could include malicious code. Avoid downloading files from sites that you do not trust. If you are getting the files from a supposedly secure site, look for a web site certificate. If you do download a file from a web site, consider saving it to your computer and manually scanning it for viruses before opening it.

**Check your phone bill monthly** - Monthly subscriptions for texting a "joke of the day" or "daily horoscope" are a common scam. Often time people don't realize they have signed up for them which is buried in the fine print of some unrelated service. You can also inform your wireless provider to block subscription services from your phone or PDA.

**Evaluate your security settings** - Make sure that you take advantage of the security features offered on your device. Attackers may take advantage of Bluetooth connections to access or download information on your device. Disable Bluetooth when you are not using it to avoid unauthorized access.

<sup>1</sup> Mindi McDowell. *Defending Cell Phones and PDAs Against Attack*, <http://www.us-cert.gov/cas/tips/ST06-007.html> (8/9/2006)

**Why Law Firms?**

- ✓ Why are law firms at risk?
  - Rich collection of confidential information
  - Security vulnerabilities
  
- ✓ Frequency of law firm data breaches
  - Lack of reporting requirements
  - Lack of technology sophistication
  - Failure to detect a breach / breaches are reported



## Why Are Small and Midsize Businesses Targeted?

- ✓ Small and midsize businesses (SMBs) are the principal target of cybercrime.
  - Based on one study, 60 percent of all targeted cyberattacks last year struck SMBs.
- ✓ SMBs are easier targets than larger organizations.
- ✓ Many SMBs lack sufficient resources and in-house expertise to address cyberattacks.
- ✓ It has been estimated that half of the small businesses that suffer a cyberattack go out of business within six months as a result.

Source: U.S. Securities and Exchange Commission, "The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses," 2015.

17

## Ethical Considerations

- ABA Formal Opinion 477 - Requires lawyers to make reasonable efforts to ensure that communications with their clients are secure and not subject to inadvertent or unauthorized cybersecurity breaches.
  - *This update of May 2017 addressed the use of tablets, smartphones and cloud storage.*
- Model Rule 1.1 – Competence - New commentary: “keep abreast of changes in the law and its practice, including the benefits and risk associated with relevant technology.”
- Model Rule 1.6 – Confidentiality – A lawyer shall not reveal information relating to the representation of a client...
- Model Rule 1.6(c) – A Lawyer shall make a reasonable effort to prevent the unintended disclosure of, or unauthorized access to, information relating to the representation of a client.
- Model Rule 1.4 – Communication – A lawyer shall keep the client informed and consult with the client about the representation.
- Model Rule 5.1, 5.2, and 5.3 – Supervision – Supervisory lawyers within a law firm have a duty to ensure that all members of the firm comply with the Rules.

18

## Regulatory Gaps

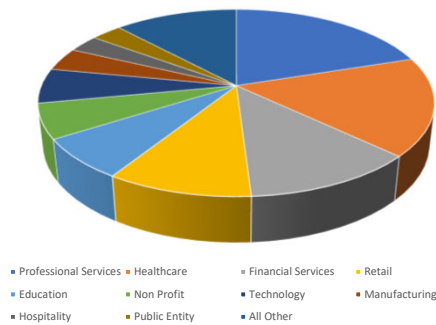
- Regulatory gaps exist because laws have not (*cannot?*) kept up with advances in technology
- Gaps are getting WIDER as technology advances more rapidly
- Laws changing/updating frequently to try to fill gaps



19

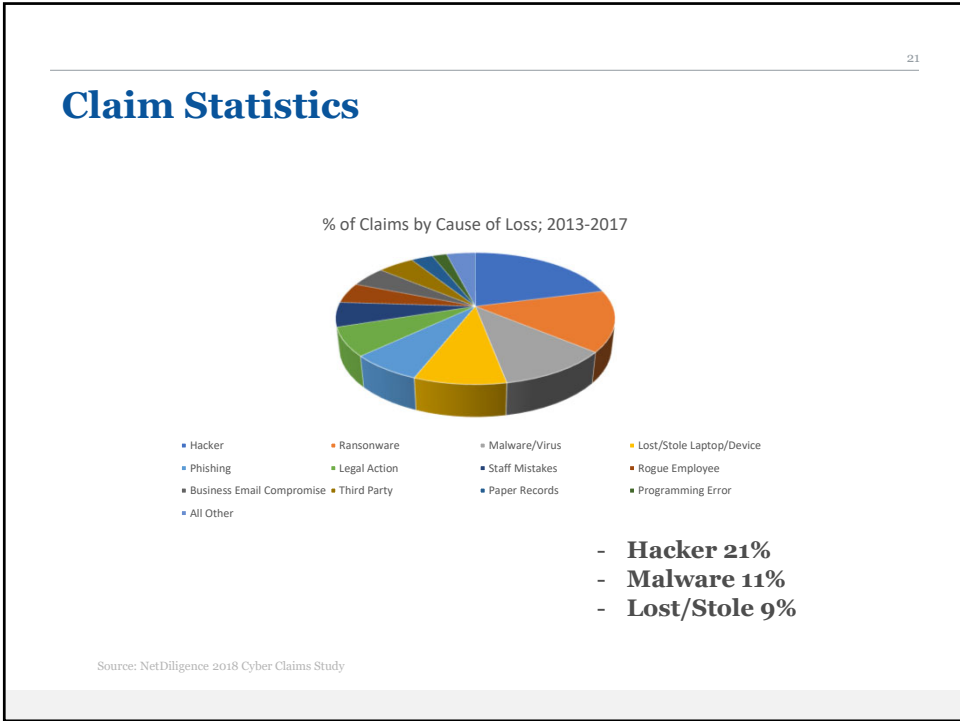
## Claim Statistics

% of Claims by Section: 2013-2017

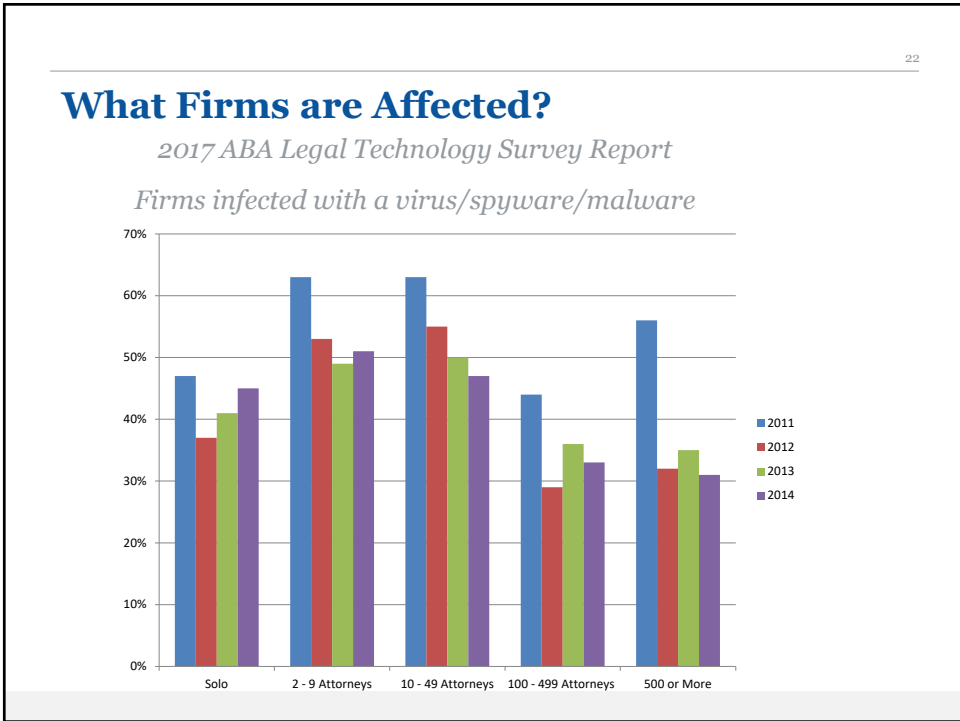


Source: NetDiligence 2018 Cyber Claims Study

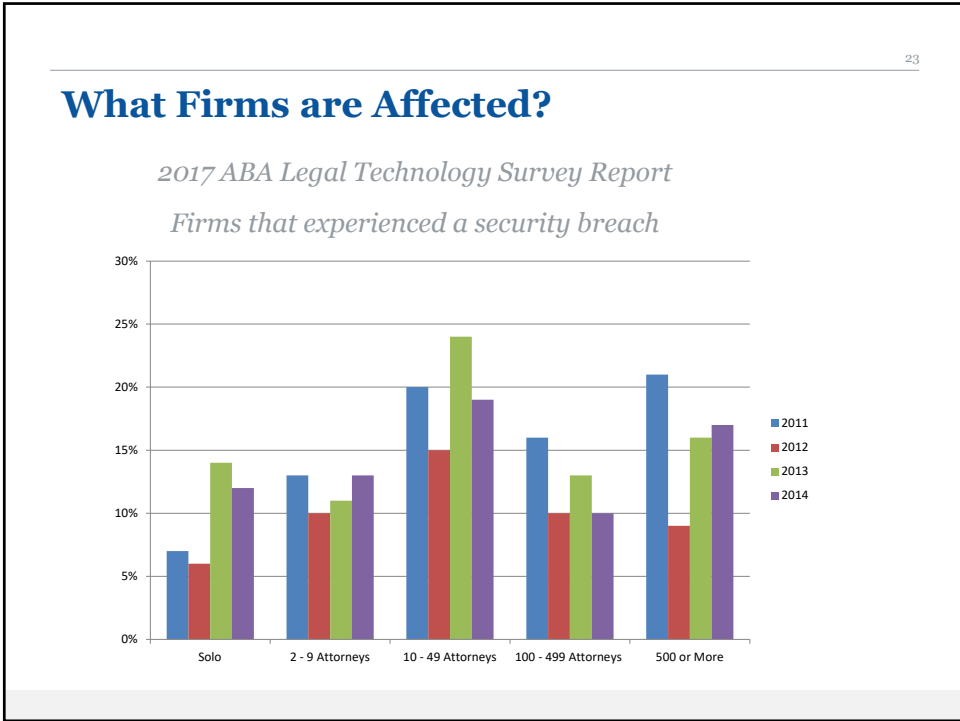
20



21



22



23

24

## Claim Statistics

Crisis Services Costs 2014–2017

	Cases	Min	Average	Median	Max
Forensics	276	265	141,479	35,175	3,860,000
Credit/ID Monitoring	118	10	112,886	5,511	2,000,000
Notification	138	14	234,011	13,323	5,520,000
Legal Guidance / Breach Coach*	341	112	53,133	14,922	2,500,000
Other	71	149	80,643	10,295	2,000,000
<b>Total Crisis</b>	<b>446</b>	<b>14</b>	<b>248,980</b>	<b>35,577</b>	<b>8,209,000</b>

Source: NetDiligence 2017 Cyber Claims Study

24

25

## Claim Statistics

**Legal Costs—Damages Defense & Settlement 2014–2017**

	Cases	Min	Average	Median	Max
<b>Legal Damages Defense</b>	64	319	120,606	15,500	2,500,000
<b>Legal Damages Settlement</b>	37	1,502	254,851	50,000	4,800,000

**Legal Costs—Regulatory Defense & Fines 2014–2017**

	Cases	Min	Average	Median	Max
<b>Regulatory Action Defense</b>	10	25,163	696,524	83,750	5,791,000
<b>Regulatory Action Fines</b>	2	28,943	44,634	44,634	60,324

Source: NetDiligence 2017 Cyber Claims Study

25

26

## Data Security Gaps

- ✓ Lost or stolen devices
- ✓ Wireless access
- ✓ Plain text email
- ✓ Vendor management
- ✓ Staff training
- ✓ Insider threats
- ✓ Cloud computing
- ✓ Encryption

26

27

## Demand and Drivers for Cyber Insurance

- Demand for Cyber Insurance
  - Most insurance carriers have reported experiencing an increase in demand
  - Need for additional capacity
  - Policy terms and conditions are broadening
  - Additional sublimited coverage being offered
  
- Drivers for Cyber Insurance
  - Privacy Notification Laws
  - News of cyber-related events
  - Board/Sr. Management
  - Increased education
  - Experiencing a cyber-related loss
  - Contractual obligations

27

28

## Insurance Coverage Gaps

	Property	General Liability	Crime/Bond	K&R	E&O	Cyber / Privacy
<b>1st Party Privacy / Network Risks</b>						
<i>Physical Damage to Data</i>						
<i>Virus/Hacker Damage to Data</i>						
<i>Denial of Service attack</i>						
<i>B.I. Loss from Security Event</i>						
<i>Extortion or Threat</i>						
<i>Employee Sabotage</i>						
<b>3rd Party Privacy/Network Risks</b>						
<i>Theft/Disclosure of private info</i>						
<i>Confidential Corporate Breach</i>						
<i>Technology E&amp;O</i>						
<i>Media Liability (electronic content)</i>						
<i>Privacy Breach Expense</i>						
<i>Damage to 3rd Party's Data</i>						
<i>Regulatory Privacy Defense/Fines</i>						
<i>Virus/ Malicious Code Transmission</i>						

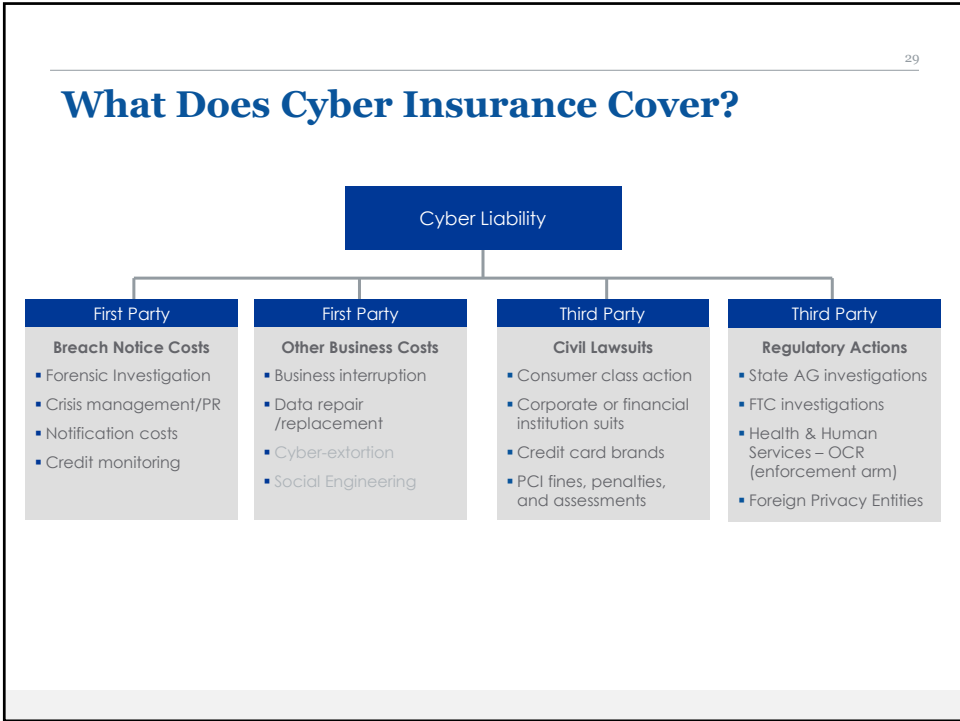
Coverage Provided:	
Limited Coverage:	
No Coverage:	

**Traditional Insurance Gaps to name a few:**

- Theft or disclosure of Third Party Information – GL
- Security & Privacy – “intentional act” exclusion – GL
- Data is not tangible Property – GL, Prop. and Crime
- Bi/PD Triggers – GL
- Value of Data if corrupted, destroyed or disclosed – Prop & GL
- Contingent Risks from external hosting, etc .

- Commercial Crime policies require “intent” and only cover “money securities and other Tangible Property”
- Territorial Restrictions
- Sublimits or long waiting periods applicable to any virus coverage available – Prop.

28



29

- 30
- ## What is NOT COVERED by Cyber Insurance?
- ✓ Theft of Corporate Intellectual Property or Trade Secrets
  - ✓ Brand Damage
  - ✓ Loss of Future Revenue
    - As in the case of Target, for example, if sales were down due to customers staying away after data breach
  - ✓ Negligence/Induced Incidents
  - ✓ Nation State Attacks (excluded)
  - ✓ Improved IT Security Measures (post breach remediation)
  - ✓ Physical Damage

30

## Critical Coverage Issues

- Choice of counsel
- Choice of third-party vendors
- Delete exclusions
  - Lack of patch upgrades/unencrypted data/devices
- Incident caused by a third-party vendor
- Allocation of coverage between necessary remediation costs and relative upgrades
- Extra costs incurred due to complying with a government order to take (or not take) certain actions to stop the incident
- “GDPR Endorsements”
- Definitions: Privacy Regulation/Law; Personal Information; Privacy Regulatory Proceeding (just proceeding or investigation/inquiry)
- Wrongful Collection Exclusions (“Spam” Exclusions) need to be addressed.