Cybersecurity Issues in Bankruptcy Law

1

Disclaimer

This video may be construed as attorney advertising under Rule 7.3(a)(1) of the New York State of Professional Responsibility and is provided pursuant to section 7.3(r): "Without affecting the right to accept employment, a lawyer may speak publicly or write for publication on legal topics so long as the lawyer does not undertake to give individual advice."

2

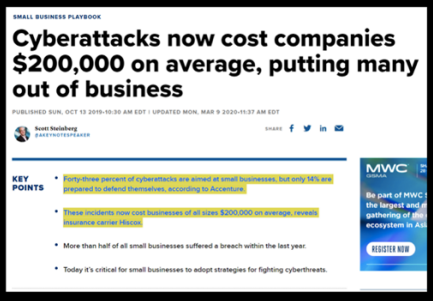
TOPICS OF DISCUSSION

1. Cybersecurity Breaches resulting in Bankruptcy
   - Bankruptcy filings resulting from Cybersecurity breach
   - Time to terminal impact
2. Cyberthreat resulting from Technology Service Suppliers Filing for Bankruptcies
3. The intersection between cybersecurity and privacy issues and insolvency issues
   - Before distress
   - To accept or reject an executory contract?
   - Post-confirmation preservation and access
4. Getting your law firm in compliance with cyber security responsibilities

3

Cybersecurity Breaches resulting in Bankruptcy

4



SMALL BUSINESS PLAYBOOK

Cyberattacks now cost companies $200,000 on average, putting many out of business

PUBLISHED SUN, OCT 13 2019-10:30 AM EDT | UPDATED MON, MAR 9 2020-11:37 AM EDT

Scott Steinberg
FAKEYOUTEPRAKER

SHARE

KEY POINTS

- Forty-three percent of cyberattacks are aimed at small businesses, but only 14% are prepared to defend themselves, according to Accenture.
- These incidents now cost businesses of all sizes $200,000 on average, reveals insurance carrier Hiscox.
- More than half of all small businesses suffered a breach within the last year.
- Today it's critical for small businesses to adopt strategies for fighting cyberthreats.

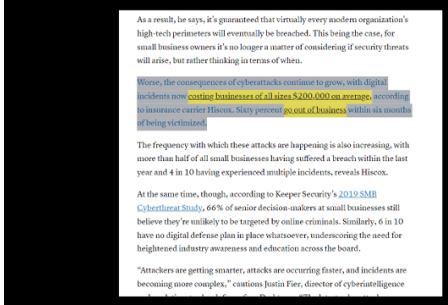
MWC

Be part of MWC the largest and gathering of ecosystem in As

REGISTER NOW

Source: https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

5



As a result, he says, it's guaranteed that virtually every modern organization's high-tech perimeters will eventually be breached. This being the case, for small business owners it's no longer a matter of considering if security threats will arise, but rather thinking in terms of when.

Worse, the consequences of cyberattacks continue to grow, with digital incidents now costing businesses of all sizes $200,000 on average, according to insurance carrier Hiscox. Sixty percent go out of business within six months of being victimized.

The frequency with which these attacks are happening is also increasing, with more than half of all small businesses having suffered a breach within the last year and 4 in 10 having experienced multiple incidents, reveals Hiscox.

At the same time, though, according to Keeper Security's 2019 SMB Cyberthreat Study, 66% of senior decision-makers at small businesses still believe they're unlikely to be targeted by online criminals. Similarly, 6 in 10 have no digital defense plan in place whatsoever, underscoring the need for heightened industry awareness and education across the board.

"Attackers are getting smarter, attacks are occurring faster, and incidents are becoming more complex," cautions Justin Fier, director of cyberintelligence

Source: https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

6

Time to terminal impact

7

From Breach to Bankruptcy – How the Terminal Impact of Cyber Attacks is Accelerating

Peter Cohen
Managing Director - EMEA at HolistiCyber

19 articles + Follow

April 8, 2018

The time it takes for firms to go out of business due to cyber attack is decreasing. In 2000 it took ten years, in 2017 it took just eight months. In fact, since 2010 the cyber attack 'time to Terminal Impact' (bankruptcy) has pretty much halved every two years in a twisted inversion of **Moore's Law**.

https://www.linkedin.com/pulse/from-breach-bankruptcy-how-terminal-impact-cyber-attacks-peter-cohen/

8

The cyber security industry likes to pin this impact on the evolution of 'the threat', but in reality there's a lot more to it. Yes the threat is evolving, continually and rapidly, but this simply keeps it capable of overcoming whatever preventative controls are in place at the time. As such, the threat generally evolves to stay 'good enough to effect a breach' and although there are exceptions, at a macro level it can be considered a relative constant.

What are not a relative constants, and what are the primary causes for the decrease in time to terminal impact, are the ways in which we do business and communicate. Across every industry the drive to be digital, agile, and data-led has enabled our economies and companies to unlock huge productivity and innovation gains. However, these gains come with a hidden cost, as it has become:

- Quicker to gain value from stolen IP
- Easier for customers to switch and go elsewhere
- Quicker for news to travel
- Faster to perform financial transactions

The following examples are among the only cyber-related bankruptcies in firms of a significant size (worth over $100m or with $100m in assets at the time of the breach.). Their stories are indicative of an acceleration towards terminal impact.

https://www.linkedin.com/pulse/from-breach-bankruptcy-how-terminal-impact-cyber-attacks-peter-cohen/

9

Nortel Networks (10 years to Terminal Impact)

In the year 2000, Nortel Networks had an annual revenue of $30 billion. One of the world's largest technology companies, Nortel won $40 of every $100 spent on telecoms and networking in the US, and had a vast global footprint. In 2004 it was discovered that some computers were sending regular data transmissions to China, although the extent of the breach was only mapped out in 2009. Further investigation revealed that the Nortel had undergone systematic and continuous data exfiltration over a 10 year period. This led to a complete loss of competitive advantage, with IP, R&D and business planning data accessed and removed.

Despite the hack being traced to China, Beijing deny involvement with the attack and has never been formally implicated. However, in clear contrast to Nortel's fate it is perhaps worth touching on Huawei's meteoric rise from small reseller in 1990 with little IP, to achieving annual telecom and networking revenues of $22 billion in 2009 – with 75% of its sales in Nortel's traditional strongholds.

Breached in 2000, Nortel hit terminal impact through filing for bankruptcy in 2009.

https://www.linkedin.com/pulse/from-breach-bankruptcy-how-terminal-impact-cyber-attacks-peter-cohen/

10

SolarWorld (5 years to Terminal Impact)

Once the world's leading supplier of solar panels, SolarWorld were primed in 2012 to take advantage of the green energy revolution through heavy investments in research, development and the solar manufacturing process. It didn't quite turn out that way, with the firm filing for bankruptcy in 2017, **five years after they were hacked by Chinese attack group APT1**. The US Justice Department indictments states that IP, the manufacturing process and key financial data was stolen in order to:

- a) replicate the SolarWorld technology, and
- b) determine the length of time it would take for SolarWorld to go out of business if the market was flooded with cheap replicas

We know now how long that was – five years. In that time, China have become the world's pre-eminent solar manufacturer and energy producer, smashing its own 2020 targets in 2017 – the same year SolarWorld went bankrupt.

https://www.linkedin.com/pulse/from-breach-bankruptcy-how-terminal-impact-cyber-attacks-peter-cohen/

11

Mossack Fonseca (2.5 years to Terminal Impact)

In 2016, Mossack Fonseca represented 300,000 companies, and with 600 staff in 42 countries were the world's fourth largest offshore legal specialist. Due to the nature of its work in handling high-net worth transactions and tax efficient schemes, clients relied on it for confidentiality and complete discretion. As such, its reputation was everything, and could be considered to be its most critical asset. The Mossack Fonseca breach was effected in 2015 by an unknown threat actor, motivated by exposing the work the firm carried out on behalf of its high-net worth clients. 11 million files were exfiltrated and then passed to an investigative journalist consortium.

In 2016 that asset – reputation – was shattered forever; the '**Panama Papers**' were published detailing client data with full disclosure as to who was moving what money, and where – causing a media storm that quickly went global. The nature of the story and the persistence which it carried online and in print and broadcast was meant that terminal impact was relatively swift. While it didn't go bankrupt, Mossack Fonseca has undergone near-complete client loss leading to a series of office closures, with its last 50 staff leaving in March 2018 as the business was wound up.

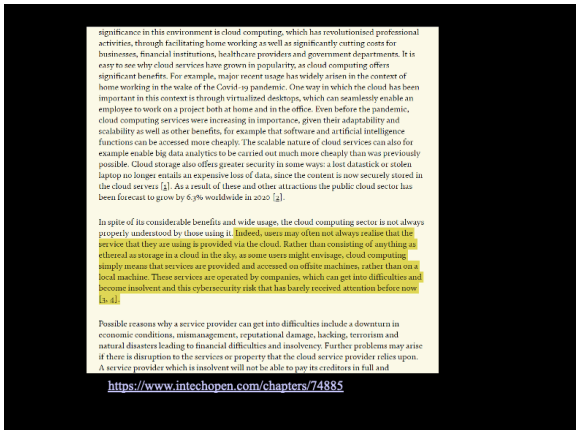
https://www.linkedin.com/pulse/from-breach-bankruptcy-how-terminal-impact-cyber-attacks-peter-cohen/

12

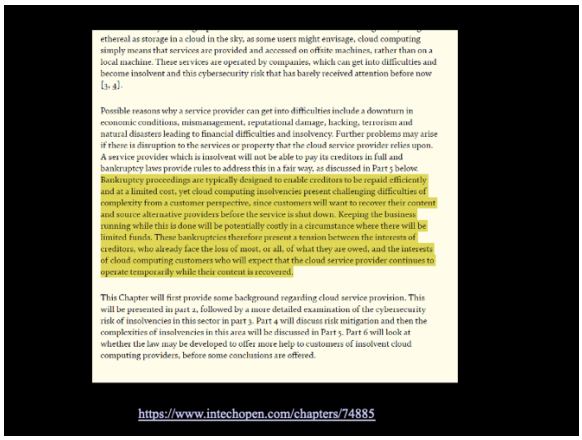
13

14

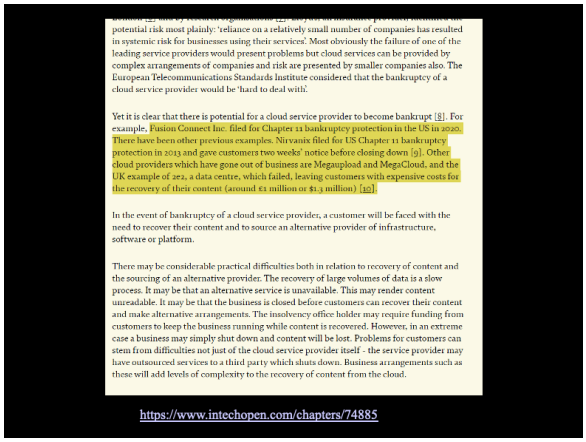
15



16.



17



18.

There have been other previous examples. Nirvanix filed for US Chapter 11 bankruptcy protection in 2013 and gave customers two weeks' notice before closing down [9]. Other cloud providers which have gone out of business are Megaupload and MegaCloud, and the UK example of 2e2, a data centre, which failed, leaving customers with expensive costs for the recovery of their content (around £1 million or $1.3 million) [10].

In the event of bankruptcy of a cloud service provider, a customer will be faced with the need to recover their content and to source an alternative provider of infrastructure, software or platform.

There may be considerable practical difficulties both in relation to recovery of content and the sourcing of an alternative provider. The recovery of large volumes of data is a slow process. It may be that an alternative service is unavailable. This may render content unreadable. It may be that the business is closed before customers can recover their content and make alternative arrangements. The insolvency office holder may require funding from customers to keep the business running while content is recovered. However, in an extreme case a business may simply shut down and content will be lost. Problems for customers can stem from difficulties not just of the cloud service provider itself - the service provider may have outsourced services to a third party which shuts down. Business arrangements such as these will add levels of complexity to the recovery of content from the cloud.

The potential difficulties for customers in recovering content from a cloud service provider insolvency will be considered in more detail in part 5 below.

19

4. Mitigation of the risk

The main steps that customers can take relate to diligence in selecting a cloud service provider and, where possible, the inclusion of terms in the agreement with the service provider to protect the customer's content in the event of insolvency. However, customers would also be wise to have an alternative plan in the event of a loss of content or access to software. Regular backups with a third-party provider would be one option, although not perfect, since any backup will be a snapshot of the content at the time of the most recent backup.

4.1 Assessment of supplier viability

Given the potential risk, what can customers do to protect themselves from the risk of cloud service provider insolvencies? Users would be wise to consider the potential long-term viability of cloud service providers before entering into a contract with them [11], in particular if the provider will be storing or processing data, or supplying access to important software. Large market players in the cloud service industry may offer greater prospects of longevity of supply but fewer prospects of a bespoke service. Not all customers will realistically be able to bargain with cloud service providers, as discussed below. However, some sectors such as banking [12, 13] may place pre-conditions on eligibility for cloud service providers and large customers for example [14] may also have specifications for eligible suppliers.

It would be prudent as well to identify potential alternative service providers in the event that the worst happens and selected provider can no longer offer the contracted service, denying access to data or to critical software.

20

4.2 Contractual bargaining

Cloud computing customers may try to address the risks of insolvency contractually [15, 16] however there are limitations to the effectiveness of this. For many customers, service will be on standard terms that will contain no provision for insolvency [17]. Large companies may have more negotiating power. In the event that a customer can bargain to obtain contractual protection, it will be important to clarify that there is a distinction between the ownership of the cloud infrastructure and the ownership of content in the cloud, such as data, so that the data does not form part of the bankruptcy estate [18], as discussed in the next section. Other options would be to include:

Step-in rights: entitlements that are common in outsourcing contracts and enable control to be taken of the service provider. In the cloud computing context difficulties in exercising such powers would arise where there is shared infrastructure, staff and technology.

Software escrow is another approach, which can be of benefit to customers who access software via the cloud. Under such an arrangement a third party would hold the software source code under a software escrow arrangement and release it upon the occurrence of a triggering event, which could include the insolvency of the service provider [19].

A further example is copyright splitting [20], but this might be practicably difficult to implement in the event that there are numerous users of the software.

These approaches can potentially provide workable approaches in the event of a cloud service provider insolvency.

21

5. A concise overview of bankruptcy possibilities and their consequences

In the event that a cloud service provider gets into financial difficulties there are normally two main formal insolvency possibilities that can be used to address the company's inability to pay its debts. Most simply, the cloud service provider may be liquidated or it may be reorganised, both of which procedures will be explained below. It must be added, however that the procedures that apply in the event of insolvency are not international and they will vary depending on the country in which the proceedings are opened. This presents a complication in the case of cloud service providers, which may have supranational affairs. The proper venue in which to open insolvency proceedings may be unclear, although both the US and UK are jurisdictions with well-developed insolvency frameworks, and which both take fairly expansive approaches to jurisdiction to open insolvency proceedings [21, 22] and it may be that these will be favoured as venues in cases where there is some connection with the cloud service provider.

We can illustrate the main likely insolvency procedures and issues that may arise in this context by reference to those which operate in the US and UK. As noted, both of these countries have well-developed insolvency laws. However, insolvency laws in other countries may be more limited and so may the infrastructure to deal with proceedings in respect of insolvent cloud service providers, since courts may be over-burdened and lacking in specialist expertise and insolvency professionals may lack experience and sometimes integrity. Again, these factors may hamper efforts to recover content from the cloud since there may not be a vehicle to support a managed closedown of the company's affairs. Indeed, the sophistication of the US and UK systems does not guarantee this steady closure and customers may lose their cloud content, infrastructure, platform or software.

22

5.1 Liquidation

The process of liquidation is normally used to bring the affairs of an insolvent company to an end, with an impartial trustee (in the UK a liquidator) being appointed to do this according to detailed procedures set out in laws. Examples are the United States Chapter 7 and the UK Insolvency Act 1986, Part IV. This section will initially consider the United States position before briefly examining the position in the UK. Claims by customers of cloud computing services can potentially give rise to complexities in both jurisdictions that can only be briefly touched upon.

The opening of Chapter 7 liquidation proceedings, an accessible introduction to which can be found at [23], will give rise to an automatic stay under 11 United States Code § 362 (hereafter "USC") to prevent creditors from taking action to enforce their claims and this gives temporary protection to the debtor while the liquidation is carried out. This is however a time of vulnerability for customers since the trustee, when appointed, may not realise that the company operates a cloud service on which customers depend and may fail to take steps to ensure continuity of service, in particular since funds to do so may be lacking. Even where the trustee takes steps to continue service, s/he may lack specialist skills and experience to operate a cloud service business and may face a steep learning curve in relation to the business, combined with a lean staffing structure and high volume of communications from concerned customers. Moreover, liquidation is not primarily a vehicle to enable ongoing trading. In the US, the business may continue to operate if it is in "the best interest of the estate and consistent with the orderly liquidation of the estate" under 11 USC §721 and this might feasibly enable a temporary operation of the company to enable customer needs to be attended to. There is a risk however that there may be insufficient funds to enable the trustee to continue to operate the business for long enough to enable customers to recover their content and it may be necessary for customers to provide funds if this is to be done.

23

operate a cloud service business and may face a steep learning curve in relation to the business, combined with a lean staffing structure and high volume of communications from concerned customers. Moreover, liquidation is not primarily a vehicle to enable ongoing trading. In the US, the business may continue to operate if it is in "the best interest of the estate and consistent with the orderly liquidation of the estate" under 11 USC §721 and this might feasibly enable a temporary operation of the company to enable customer needs to be attended to. There is a risk however that there may be insufficient funds to enable the trustee to continue to operate the business for long enough to enable customers to recover their content and it may be necessary for customers to provide funds if this is to be done.

The main role of the trustee will be to take steps to bring the company's affairs to an end by selling the company's assets and using the proceeds to pay off creditors, as far as possible, according to a system of priorities and customers claims will be dealt with as part of this. Since the trustee is dealing with the debtor's property it will be important for customers to establish their entitlement to the content that they have uploaded, so that it is not included in the estate that the trustee will be looking to sell. Preferably the customer's ownership of content should have been agreed in any contract with the cloud service provider, although the customer's ownership of the content is likely to be implied even if the contract does not address the point.

As to the distribution of assets in the liquidation, there is a distinction to be drawn between creditors with claims to specific property, such as items covered by a lien, and those without. The former are known as secured creditors and the latter as unsecured creditors. Unsecured creditors are further divided into those with priority and nonpriority status. In view of the secured creditors' claims to specific assets, or classes of assets, these assets do not form part of the estate for distribution to creditors. Similarly, customers with ownership of the content uploaded to the cloud are entitled to recover the content, since it does not form part of the estate, but this may be more difficult in practical terms, as discussed elsewhere in this Chapter. Unsecured creditors, in contrast, typically occupy a low level of priority.

As previously noted, there are two types: priority unsecured and nonpriority unsecured. The priority claims, such as the costs of running the bankruptcy, are to be paid first, so that nonpriority claims may have limited prospects for payment. The class of nonpriority unsecured creditors would be those with claims to damages. These might include cloud service customers whose service contracts have been prematurely discontinued, or who

24

secured creditors' claims to specific assets, or classes of assets, these assets do not form part of the estate for distribution to creditors. Similarly, customers with ownership of the content uploaded to the cloud are entitled to recover the content, since it does not form part of the estate, but this may be more difficult in practical terms, as discussed elsewhere in this Chapter. Unsecured creditors, in contrast, typically occupy a low level of priority.

As previously noted, there are two types: priority unsecured and nonpriority unsecured. The priority claims, such as the costs of running the bankruptcy, are to be paid first, so that nonpriority claims may have limited prospects for payment. The class of nonpriority unsecured creditors would be those with claims to damages. These might include cloud service customers whose service contracts have been prematurely discontinued, or who obtain a copy of the software, s/he merely accesses it online.

It is important to look in a little more detail at the claims that customers may have based on service agreements and how they will fare in the bankruptcy. In the liquidation these will be regarded as executory contracts [24] under 11 USC § 365(a), since both parties have ongoing performance obligations at the time of the bankruptcy filing and, as such, the trustee can choose whether or not to continue performance. If the trustee elects to discontinue performance the customer will have merely a claim to damages, which, as discussed in the previous paragraph, is likely to be worthless in the liquidation, and their access to content may be lost. Similar considerations apply in relation to software licences that customers hold, however there are additional protections under 11 USC §365(n) for customers in this instance, since customers can elect to retain rights under the contract to the software and its embodiments, including source code. This does not however require the liquidator to perform any of the licensor's obligations, such as updating the software, which can present problems for customers unless and until a replacement provider can be found, or unless the liquidator assigns the software to a third party capable of continuing service. Nor are all cloud computing services necessarily protected by this provision, since not all will have the character of software licences, even SAAS contracts, since the customer does not necessarily

25

previous paragraph, is likely to be worthless in the liquidation, and their access to content may be lost. Similar considerations apply in relation to software licences that customers hold, however there are additional protections under 11 USC §365(n) for customers in this instance, since customers can elect to retain rights under the contract to the software and its embodiments, including source code. This does not however require the liquidator to perform any of the licensor's obligations, such as updating the software, which can present problems for customers unless and until a replacement provider can be found, or unless the liquidator assigns the software to a third party capable of continuing service. Nor are all cloud computing services necessarily protected by this provision, since not all will have the character of software licences, even SAAS contracts, since the customer does not necessarily obtain a copy of the software, s/he merely accesses it online.

Ongoing trading in liquidation is also potentially difficult in the UK as similar issues will arise. Under the legislation, the liquidator of a company may continue to carry on business "so far as may be necessary for its beneficial winding up", according to Insolvency Act 1986, Sch 4, para 5, but this does not guarantee that there will be ongoing trading or that any period of ongoing trading will again be long enough to enable customers to recover their content and make alternative arrangements. In addition to the practical problems noted in the US context, the liquidator is not obliged to honour customers' service agreements and the liquidator has powers under Insolvency Act 1986, s 178 to disclaim unprofitable contracts, which could include cloud service agreements. Where the customer benefits from a software licence one possibility is that the liquidator will prefer to assign the software to a third party, in which case this third party will normally be subject to the licence, see further [25].

26

5.2 Reorganisation

Reorganisation, on the other hand, is designed to enable ongoing trading, through the restructuring of the debtor's financial obligations. Notable examples are the US Chapter 11 and the UK administration. There are great variations in reorganisation laws globally and some jurisdictions as yet lack suitable procedures. The main objective of reorganisation proceedings is to enable struggling but viable companies to recover from their difficulties, although these procedures are not always used to achieved this. Often reorganisation is used to enable the sale of the company's underlying business, prior to a liquidation of the company, or to otherwise enable greater returns to be made to creditors in liquidation.

Taking the US Chapter 11 as a well-developed system of reorganisation proceedings, the company's management will become what is termed a "debtor in possession", under 11 USC §1101(1), unless a trustee is appointed. Briefly, this means that the company's pre-Chapter 11 management will remain in control, with or without personnel changes. The debtor in possession will formulate a plan of reorganisation, which must be approved by creditors and by the court, and this can enable the debtor to continue trading. The debtor in possession has the power to reject contracts, as discussed in relation to liquidation. A valuable feature of Chapter 11, which also applies in Chapter 7, is the automatic stay in 11 USC § 362 and this will protect the cloud service provider from debt collection efforts by creditors, including lawsuits. Chapter 11 therefore may offer better prospects of continue trading but it is also a relatively expensive process that is used in only a small minority of insolvencies in the US.

A new UK procedure, the restructuring plan, is similar to Chapter 11 and would be suitable for larger companies which have viable prospects of recovery from their difficulties. In the UK there is also a more simple option, the company voluntary arrangement in Insolvency Act 1986, Part 1, which enables a company to reach agreement with creditors or members and does not need to be presented to a court for approval. However, the company voluntary arrangement does not provide the company with a moratorium/automatic stay on creditor claims.

27

greater returns to creditors than would be possible in an immediate liquidation. Administration is not particularly well suited to a managed closedown of a cloud service provider since an appointment must be reasonably likely to achieve the purpose of administration, set out in Insolvency Act 1986, Sch 1b, para 3. The primary purpose of administration is to save the company but if this is not reasonably practicable efforts can be focused on achieving a better return for creditors than would be likely if it was closed down without first going into administration, or if that is not reasonably practicable to make a distribution to one or more secured or preferential creditors. Since the managed closedown of a cloud service provider would be likely to add costs without benefit to creditors it is this latter objective that would need to be relied on but there is a difficulty that the administrator must 'perform his functions in the interests of the company's creditors as a whole' and the costs of a managed closedown may reduce the sums available for creditors.

Protection can alternatively be obtained via a new procedure, the restructuring moratorium, under Insolvency Act 1986, Part 2A, which offers a cheaper option than administration but potentially a shorter duration of protection. The restructuring moratorium was introduced as part of package of reforms in the wake of the Covid-19 crisis. It enables an eligible company to enjoy the benefit of a holiday from creditor claims while under the supervision of a monitor. The protection offered will be relatively brief, lasting for an initial 20 business days, although this period can be extended. Under the process for obtaining a moratorium where the cloud service provider is not subject to a winding up petition the directors are required to file documents that indicate that the company is insolvent or approaching insolvency and that the company has likely prospects of being rescued as a going concern. It is this latter requirement that would prevent this route being used for a managed closedown of a cloud service provider. A cloud service provider which is subject to a winding up petition will only be able to obtain a moratorium following an order from the court in circumstances where this will provide a better result for the company's creditors as a whole than would be possible if the company were to be wound up without an initial period of moratorium protection. Since a managed closedown primarily is required for the benefit of customers it may be difficult to argue that it would be for the benefit of creditors as a whole.

It is a weakness that there is arguably a present lack of a reorganisation procedure in the UK that can be used to temporarily facilitate ongoing trading for the managed closedown of a

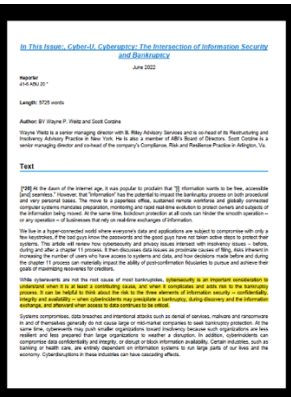
28

This Chapter has provided a brief introduction to a threat to cybersecurity that has as yet received only limited attention. The potential for cloud computing insolvencies is globally significant, given the rapidly rising usage and value of content that is stored in the cloud. Importance also arises from the growth of digital economies in many countries, including developing countries, and it would be desirable for domestic laws to pay attention to this matter. The Chapter has discussed in brief how insolvencies in this sector might be handled in the US and UK and has highlighted problems that would be faced by customers of insolvent cloud service providers. Even these sophisticated jurisdictions do not presently provide effective protection for cloud service customers. It is moreover doubtful that domestic insolvency procedures alone will ever be adequate to address failures in this sector, which is supranational in nature. There is arguably a need for discussion at a global level of how cloud computing insolvencies can be addressed, and how improvements can be made to the infrastructure to support this. There is also a need to identify if there are any other complex areas of supranational technology that will have potential for significant impact of insolvencies, since similar issues are likely to arise in other cases of service supply. This Chapter has focused on cloud computing as there is here a clearly identified risk of insolvency having a significant impact and a need for legislative attention to be paid. In the longer term the development of robust laws to handle cloud computing insolvencies requires collaboration between data scientists and insolvency lawyers and attention on a global scale.

29

The Intersection of Cybersecurity and Privacy Issues With Insolvency Issues

30



In This Issue:, Cyber-U, Cyberuptcy: The Intersection of Information Security and Bankruptcy, 41-6 ABIJ 20

31

41-6 ABIJ 20, *20

Cyber-risk during bankruptcy might be caused by the sharing of information by multiple parties with distinct interests across system configurations that range from secured, collaborative data transmission and storage platforms to everyday unencrypted email exchanges. The more players at the table, the greater the risk to the confidentiality of documents and artifacts, and possibly document integrity. Document production can be impeded if eDiscovery systems are somehow compromised.

Before Distress

A 2019 article [1] acknowledges that large companies rarely declare bankruptcy immediately after suffering a cyberattack, but instead suffer financial repercussions, embarrassing disclosures, reputational impacts and senior-management purges. First-party costs associated with credit-monitoring, notice, incident response and forensics, and stakeholder communications can be meaningful to the extent that they exceed limits, exclusions and self-funded retentions imposed by the cybersecurity insurance policy. However, it is the contingent costs not covered by insurance that may be the more important impact: shareholder (and partner/customer) derivative lawsuits, ever-more punitive regulatory enforcement actions and penalties, disruptions of business operations, and the brand/image damage that often results in the replacement of C-suite members. It might not rise to the level of bankruptcy, but the cumulative damage can be reflected in market cap devaluation, reduced deal value in M&A, intense regulatory scrutiny, and tougher contractual demands of counterparties.

When North Korean hackers (purportedly) took confidential data from Sony Pictures in 2014, they acquired personally identifiable information, emails and executive salary data. However, that paled by comparison to the damage done by making public copies of then-unreleased films, plans for future films, and scripts -- representing future enterprise **[*21]** value and competitive advantage. The *coup de grace* was that the attackers introduced a variant of the Shamoon wiper malware that essentially erased Sony's computer infrastructure, requiring a months-long rebuild of the entire IT environment, during which Sony Pictures was forced to revert to analog operations. In December 2014, a *Wall Street Journal* article estimated that the cost to Sony of the North Korean data breach would ultimately exceed $ 100 million, a figure with the potential to render many companies insolvent.

The 2019 article's analysis identified three notable companies that ceased operations due in large part to years of intellectual property (IP) theft that destroyed enterprise value: Westinghouse, Nortel Networks and SolarWorld. A pernicious form of cyberthreat, IP theft can happen in a single large data theft, but it is usually a slower and more insidious death. The theft of essential IP destroys value by compromising the basis of competitive advantage as an initial -- but not exclusive -- root cause of failure. IP theft brazenly impacts the confidentiality of information due to

In This Issue:, Cyber-U, Cyberuptcy: The Intersection of Information Security and Bankruptcy, 41-6 ABIJ 20

32

Before distress

33

companies. Smaller companies may view cyberprotection as an unaffordable luxury rather than a core cost of doing business. As a result, significant cyberevents can be the root cause of a failure that eventually leads to bankruptcy.

While IP theft may result in economic damages from which large companies can recover over time, the loss of computer systems and data can cause the demise of some organizations. In 2019, Texas-based steel structure manufacturer United Structures of America Inc. was the victim of a ransomware attack that left its financial systems locked and inaccessible. Although the company paid the ransom, they were unable to decrypt the data, began a wind-down process and ultimately filed for bankruptcy. [3]

However, not all companies are able or willing to acknowledge the extent of the risk, and in some cases the cost of adopting mitigation procedures and systems may itself be incompatible with a company's ability to operate profitably. As a practical example, consider the U.S. defense industrial base, comprised of more than 300,000 companies, most of which are small secondary or tertiary subcontractors to large prime contractors. The recent imposition of reasonable new-contract acquisition and compliance requirements for better cybersecurity, designed to protect national defense, met with a material objection from smaller contractors, united in opposition to new rules that amount to basic, sound cybersecurity.

These small contractors took the position that cybersecurity is too expensive to implement. Not surprisingly, nation-state theft and compromise of data from these small companies was the policy predicate for the new regulations in the first place. Many of these small defense contractors that resist reasonable controls risk insolvency should they be hacked, and they further jeopardize the prime contractors that depend on them, and in some cases national security.

For a chapter 11 debtor, the process itself creates risk in the areas of treatment and protection of confidential data, access to and maintenance of data and application servers on an ongoing basis to support the business and the case, and preservation of data for use once the formal bankruptcy case is resolved or a plan is confirmed.

[*56] [EDITOR'S NOTE: The page numbers of this document may appear to be out of sequence; however, this pagination accurately reflects the pagination of the original published documents.] During bankruptcy, a due-diligence process associated with a sale under § 363 or pursuant to a plan typically requires that the debtors make confidential information available to potential suitors. In the pre-connected age, sellers would set up physical data rooms containing file cabinets full of paper information, and buyers would visit these rooms in person. Access was tightly controlled, and documents generally were not permitted outside the secure location.

Connectivity and digital access have long been a double-edged sword. By allowing potential buyers to evaluate a target remotely, the universe of potential buyers increases. However, the act of making information available over

In This Issue:, Cyber-U, Cyberuptcy: The Intersection of Information Security and Bankruptcy, 41-6 ABIJ 20

34

However, not all companies are able or willing to acknowledge the extent of the risk, and in some cases the cost of adopting mitigation procedures and systems may itself be incompatible with a company's ability to operate profitably. As a practical example, consider the U.S. defense industrial base, comprised of more than 300,000 companies, most of which are small secondary or tertiary subcontractors to large prime contractors. The recent imposition of reasonable new-contract acquisition and compliance requirements for better cybersecurity, designed to protect national defense, met with a material objection from smaller contractors, united in opposition to new rules that amount to basic, sound cybersecurity.

These small contractors took the position that cybersecurity is too expensive to implement. Not surprisingly, nation-state theft and compromise of data from these small companies was the policy predicate for the new regulations in the first place. Many of these small defense contractors that resist reasonable controls risk insolvency should they be hacked, and they further jeopardize the prime contractors that depend on them, and in some cases national security.

For a chapter 11 debtor, the process itself creates risk in the areas of treatment and protection of confidential data, access to and maintenance of data and application servers on an ongoing basis to support the business and the case, and preservation of data for use once the formal bankruptcy case is resolved or a plan is confirmed.

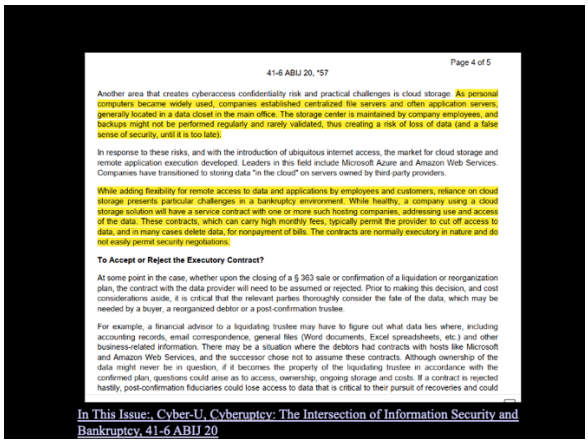
[*56] [EDITOR'S NOTE: The page numbers of this document may appear to be out of sequence; however, this pagination accurately reflects the pagination of the original published documents.] During bankruptcy, a due-diligence process associated with a sale under § 363 or pursuant to a plan typically requires that the debtors make confidential information available to potential suitors. In the pre-connected age, sellers would set up physical data rooms containing file cabinets full of paper information, and buyers would visit these rooms in person. Access was tightly controlled, and documents generally were not permitted outside the secure location.

Connectivity and digital access have long been a double-edged sword. By allowing potential buyers to evaluate a target remotely, the universe of potential buyers increases. However, the act of making information available over an internet connection greatly increases the risk of problems, including confidentiality breaches. Electronic data rooms or virtual data rooms have become the norm to address this risk, but debtors must be satisfied that the security protocols employed by the vendor are adequate. When systems are being accessed remotely, **[*57]** security is only as good as the weakest connected system and the security habit of users.

Furthermore, administrative and access rights, which are controlled by the debtor or its agent (often, an investment banker) must be set up carefully to provide only the level of access intended: read/write, edit, download, etc. Access logs should be scrutinized regularly by the debtors' advisors in order to monitor what information has been downloaded and by whom. It should go without saying that anyone accessing confidential data should be bound by an appropriate confidentiality or nondisclosure agreement. Bankruptcy-driven sales have the propensity to attract

In This Issue:, Cyber-U, Cyberuptcy: The Intersection of Information Security and Bankruptcy, 41-6 ABIJ 20

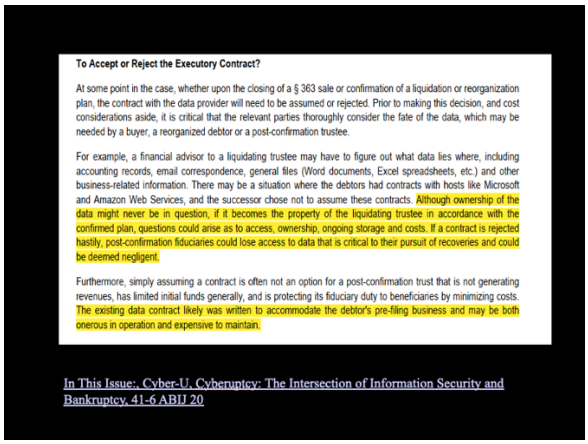
35



36

To accept or reject an executory contract?

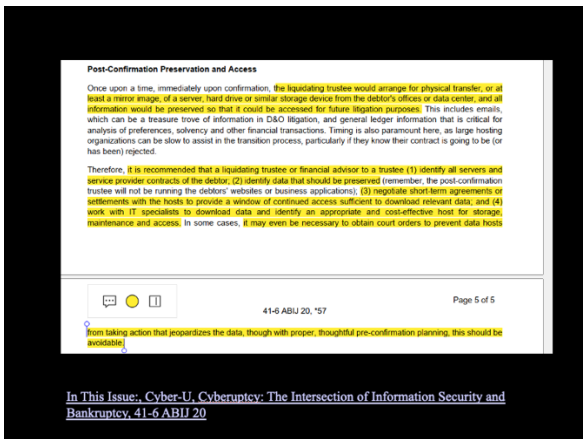
37



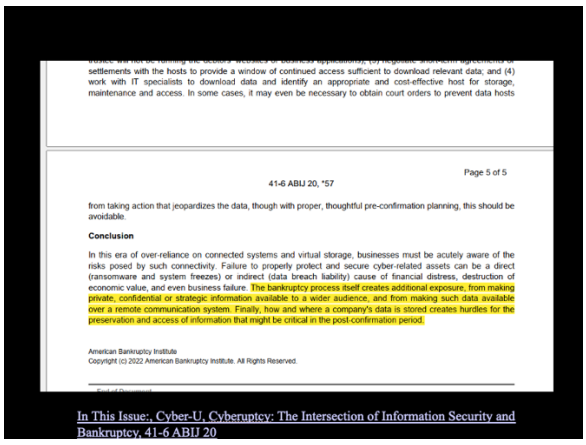
38

Post-confirmation Preservation and Access

39



40



41

How law firms can comply with ethical obligation to obtain a secure environment

42

Train the attorneys about cybersecurity

43

NEW YORK STATE CLE PROGRAM RULES

22 NYCRR 1500.22

Section 1500.22. Minimum Requirements

Currentness

<Section effective July 1, 2023. See, also, section effective until July 1, 2023.>

(a) *Credit Hours.* Each attorney shall complete a minimum of 24 credit hours of accredited continuing legal education each biennial reporting cycle in ethics and professionalism, skills, law practice management, areas of professional practice, diversity, inclusion and elimination of bias, or cybersecurity, privacy and data protection, at least four (4) credit hours of which shall be in ethics and professionalism, at least one (1) credit hour of which shall be in diversity, inclusion and elimination of bias, and at least one (1) credit hour of which shall be in cybersecurity, privacy and data protection.

Attorneys may apply a maximum of three (3) credit hours of cybersecurity, privacy and data protection-ethics to the four-credit hour ethics and professionalism requirement.

Ethics and professionalism, skills, law practice management, areas of professional practice, diversity, inclusion and elimination of bias, and cybersecurity, privacy and data protection are defined in § 1500.2.

https://www.nycourts.gov/LegacyPDFS/attorneys/cle/17b-Rules-1500-22a-Cybersecurity-Experienced-Attorney-Requirement.pdf

44

9/13/23, 1:13 PM Attorneys' Duties to Protect Client Data | Practical Law

WESTLAW CLASSIC

Attorneys' Duties to Protect Client Data

by Practical Law Data Privacy & Cybersecurity

Maintained • USA (National/Federal) Related Content

A Practice Note discussing attorneys' obligations to protect client data against security breaches under ethical rules, federal laws including the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), and Gramm-Leach-Bliley Act (GLBA), and state data breach notification and information security laws. It also discusses the potential applicability of the EU General Data Protection Regulation (GDPR) to law firms. This Note provides guidance for law firms and attorneys on how to comply with their obligations to protect client data.

https://content.next.westlaw.com/practical-law/document/Ic56d205834d911e89bf099c0ee06c731/Attorneys-Duties-to-Protect-ClientData?viewType=FullText&originationContext=document&transitionType=DocumentItem&ppcid=f7454c1138fd4cf8a473099a87debe32f&contextData=(sc.DocLink)

45

Develop and Implement a Comprehensive Information Security Program

To comply with their legal, ethical, and contractual obligations to protect client data, law firms should implement an overarching information security program documented in written information security policies.

The written information security policies should include measures to identify and address internal and external risks to information security.

However, before developing an information security program, law firms should:

- Identify applicable laws or other legal obligations, including those imposed by contract.
- Review, choose, and adopt industry standards and best practices.
- Determine whether to publish a single information security policy or multiple policy documents.
- Examine how the law firm's culture and characteristics may affect policy decisions and effectiveness.
- Consider engaging one or more independent third-party auditors or assessors to help identify their data security risks.

https://content.next.westlaw.com/practical-law/document/Ic56d205834d911e89bf099c0ee06c731/Attorneys-Duties-to-ProtectClientData?viewType=FullText&originationContext=document&transitionType=DocumentItem&ppcid=f7454c1138fd4cf8a47309a87debe32f&contextData=(sc.DocLink)

46

Developing comprehensive information security policies and programs help law firms to:

- Establish information security as a core value.
- Formulate clear rules for using and protecting PII and other sensitive information.
- Provide a basis for training and ongoing awareness building efforts.
- Foster communication among employees and the information security team.

https://content.next.westlaw.com/practical-law/document/Ic56d205834d911e89bf099c0ee06c731/Attorneys-Duties-to-ProtectClientData?viewType=FullText&originationContext=document&transitionType=DocumentItem&ppcid=f7454c1138fd4cf8a47309a87debe32f&contextData=(sc.DocLink)

47

Invest in Data Security Controls and Procedures

Law firms should invest in data security controls and procedures to prevent and detect cyberattacks. These include the most up-to-date IT protection measures, for example:

- Maintaining a current asset inventory for all computer and network hardware and software.
- Using secure configurations.
- Monitoring vulnerability reports and applying the latest security patches.
- Granting access only to those with a demonstrated business need to know.
- Protecting all passwords and other access credentials.
- Encrypting important or sensitive data and personal information.
- Using current anti-virus software and other measures to protect against malware.

https://content.next.westlaw.com/practical-law/document/Ic56d205834d911e89bf099c0ee06c731/Attorneys-Duties-to-Protect-ClientData?viewType=FullText&originationContext=document&transitionType=DocumentItem&ppcid=f7454c1138fd4cf8a47309a87debe32f&contextData=(sc.DocLink)

48

- Building security into applications and systems using security by design principles.
- Testing mobile apps, websites, and devices to identify and address potential privacy issues and security lapses.
- Developing, implementing, and maintaining sound network security architecture and controls, such as:
  - firewalls;
  - network segmentation;
  - intrusion detection and prevention services; and
  - data loss (data leakage) prevention software.
- Monitoring and managing log files to detect security incidents.
- Monitoring activities and procedures of third-party contractors with direct or remote access to the company's network and computer systems.
- Performing network scans to assess vulnerabilities.
- Monitoring activity on the network.

https://content.next.westlaw.com/practical-law/document/Ic56d205834d911e89bf099c0ee06c731/Attorneys-Duties-to-Protect-ClientData?viewType=FullText&originationContext=document&transitionType=DocumentItem&ppcid=f7454c1138fd4cf8a47309a87debe32f&contextData=(sc.DocLink)

49

Rules of professional conduct

50

Rules of Prof. Con., Rule 1.1 McK.Consol.Laws, Book 29 App.
NY ST RPC Rule 1.1

Rule 1.1. Competence

Currentness

(a) A lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

(b) A lawyer shall not handle a legal matter that the lawyer knows or should know that the lawyer is not competent to handle, without associating with a lawyer who is competent to handle it.

(c) A lawyer shall not intentionally:

(1) fail to seek the objectives of the client through reasonably available means permitted by law and these Rules; or

(2) prejudice or damage the client during the course of the representation except as permitted or required by these Rules.

https://www.nycourts.gov/ip/judicialinstitute/transgender/220E.pdf

51

Legal Knowledge and Skill

[1] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter, and whether it is feasible to associate with a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances. One such circumstance would be where the lawyer, by representations made to the client, has led the client reasonably to expect a special level of expertise in the matter undertaken by the lawyer.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kinds of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

https://www.nycourts.gov/ip/judicialinstitute/transgender/220E.pdf

52

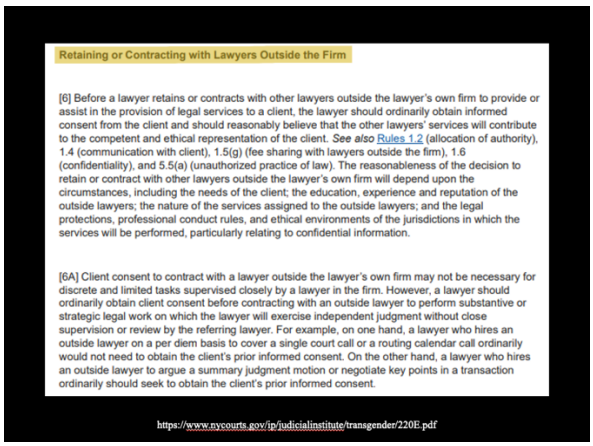
[4] A lawyer may accept representation where the requisite level of competence can be achieved by adequate preparation before handling the legal matter. This applies as well to a lawyer who is appointed as counsel for an unrepresented person.

Thoroughness and Preparation

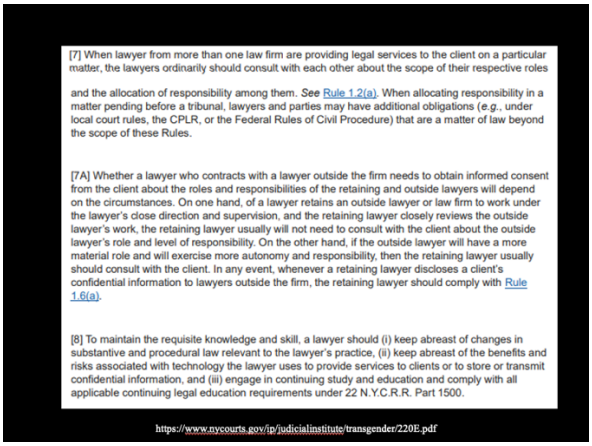
[5] Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client may limit the scope of the representation if the agreement complies with Rule 1.2(c).

https://www.nycourts.gov/ip/judicialinstitute/transgender/220E.pdf

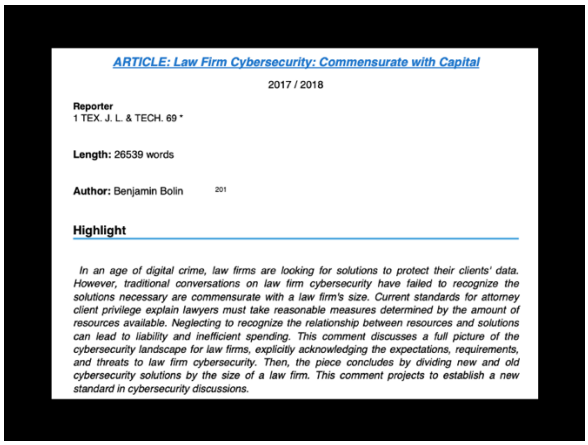
53



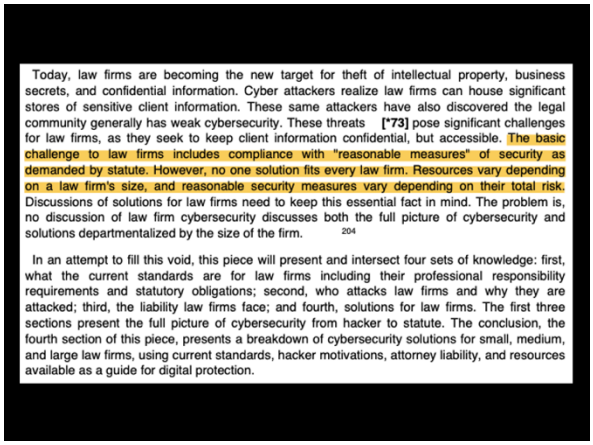
54



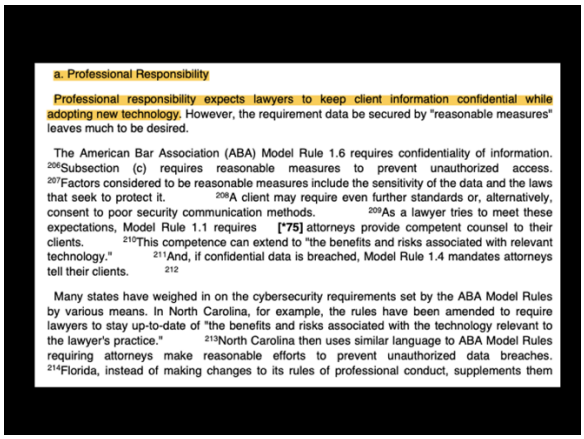
55



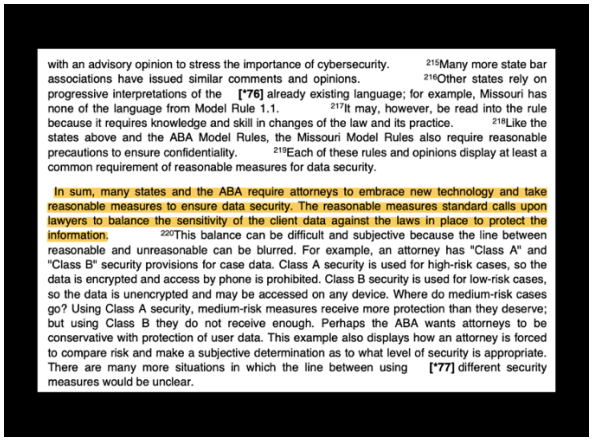
56



57



58



59

b. State Statutes

In addition to professional responsibility requirements, some state statutes have more stringent requirements. For instance, some states require notification within short timeframes if client data is breached. [221]While a minority of states require specific data security measures, some states' requirements can include encrypting all records and training employees. [222]

Forty-seven states have statutes governing data breach notification, which apply to law firms who store client data. California enacted the first notification law in 2002, and many states followed suit. [223]California, like most other states, requires entities who hold personal information about their clients to notify them upon discovery of a data breach without unreasonable delay. [224]Although most states require notification, many statutes vary widely on issues such as the timeframe in which you must notify affected persons, civil or criminal penalties, and notification of law enforcement. [225]Some states impose **[*78]** strict liability for failure to notify. [226]Additionally, some states set a capped penalty for failure to notify, while others use a calculation. [227]States like Missouri have created a "safe harbor" for data breach notification if the data was encrypted. [228]

A handful of states have enacted laws requiring data security standards to protect personal information. [229]These state laws protect against data breaches and require businesses to implement and maintain reasonable security measures similar to the requirements set for attorneys by the ABA model rules. For example, Massachusetts data privacy regulations are very comprehensive. [230]The statute requires every "person" or entity holding or

60

IV. LAW FIRM LIABILITY: A SUMMARY

After identifying the standards for law firms and who cyber attackers are, the next and greatest challenge is to acknowledge the liability present in law firms. Law firms are prime targets because they tend to have the weakest security measures for very valuable and personal information. Moreover, liability for cyberattacks will only increase as insurance coverage falls, wealth and seek to disrupt).

[*85] a. Why Law Firms?

Cyber attackers target law firms because of the high volume of data and the low level of security. Law firms do not have the same level of resources that large companies have to secure client data. This means that firms are the weakest link in the information security chain, and thus low-hanging fruit for hackers. This situation is a result of the balancing act inherent to the practice: weighing security against adoption of new technology. [262]

Hackers attack law firms for their valuable information. As established in the previous sections, a hacker's main motivation is economic or political. These motivations carry over in the attack of law firms--especially given the amount and type of sensitive information in their networks. [263]A law firm inherently deals with sensitive and personal information. Attorneys are also privileged with non-public information from businesses--whether that be a lawsuit, merger, or business secret. Much of this personal information is stored digitally in a network. A firm's network may contain information about a very large number of clients. Hackers seek non-public information on mergers and acquisition deals to get an advantage on the stock market. [264]State actors seek the information to undermine America's long-term competitiveness. [265]Inherently, law firms are a digital **[*86]** treasure trove of valuable client information.

61

b. Recent Attacks: Examples

A discussion about recent data breaches may help put into perspective why law firms are attacked. At least 80 percent of the top U.S. law firms have had their security breached by cyber attackers. [274] **[*88]** According to a 2012 report analyzing 137 events from 2009-2011, the average cost of a data breach was $ 3.7 million. [275]A Ponemon Institute report displayed the average cost of cybercrime for retail stores in 2014 was $ 8.6 million per company, which represented a double in cost from the previous year. [276]

The following true examples of cyberattacks illustrate why the liability law firms face is paramount. In 2010, the law firm Gipson Hoffman & Pancione saw their employees were receiving social engineering emails that were coming from spoofed email addresses carrying malware that could compromise the firm's security. [277]It was later discovered that the attacks emanated from China. [278]The cyberattacks methodology of using spoofed email addresses is known as "spear phishing," which is a common way to gain access to a network. [279]Spear phishing uses emails that intentionally appear to be coming from colleagues but are actually fake. Fortunately, in this case, technology-aware attorneys recognized the emails as potentially dangerous and the malware was not released. [280]

62

Cyber-security options for law firms based on law firm size

63

How small law firms can protect themselves from cyber attacks

64

a. Training

Training can prevent many cyber threats. In fact, the above discussion of the Gipson Hoffman & Pancione breach showed how training can be the last line of defense for a firm. In that situation, malware was prevented from entering the firm's system when trained lawyers identified dangerous materials. Past any or all security measures the firm may have had, well-trained lawyers stopped the threat. Trained attorneys can also help halt internal threats. During the ABA Techshow in 2014, security experts highlighted a survey that forty-one percent of IT security professionals regard "rogue" employees as a major security threat. [291]A study by Verizon found that a company's legal department is much more likely to open phishing emails than all other departments. [292]As established in the *Recent Attacks* section, these social engineering tactics are a mainstay of hackers. Ransomware is another malicious program that requires similar social engineering of employees. Despite how important training can be to the security of a law firm, in the 2016 ABA Legal **[*93]** Technology Survey, thirty percent of respondents believed their employers offered no technology training: [293]hardly better than the *2015* Legal Technology Survey. [294]For small firms, specifically, training is even less likely. Forty-five percent of solo practitioners and thirty-five percent of law firms with two to nine attorneys have no technology training program. [295]The solution to many threats both internal and external, is training. The *ABA Cybersecurity Handbook* asks firms to foster a culture of training. [296]

65

i. *Educate attorneys on the current cybersecurity threat environment.*

Trained attorneys will be on high alert for malware, spear phishing, and pesky social engineering tactics. Educate attorneys on protective measures in place to prevent attacks. Attorneys are already required to provide competent counsel, extending to benefits and risks in technology. [297]This requirement includes internal firm standards not to use external USB drives, or how the security software at the firm actively prevents cybersecurity breaches. The ABA Cybersecurity Handbook believes awareness of company policy and security measures can help attorneys negotiate contracts against unreasonable data security language. [298]

[*94] ii. *Educate attorneys to use strong unique passwords.*

Attorneys should also be trained--if not required--to change their passwords to email, their computer, and their phone frequently. Having an ineffective password on devices can leave someone dangerously exposed. [299]The passwords created should use combinations of symbols and letters or even phrases. [300]If firm employees cannot remember their passwords, train them to use programs like KeyPass, Password Safe, or other password programs, some of which are free. [301]Further, passwords and authentication are a standard set by the FTC for companies handling client data. If attorneys use no form of authentication, FTC guidelines require they change or face litigation.

66

Educate attorneys to update their computers. Non-state and individual hackers make use of security exploits in older versions of software. Updating software and applications closes those security holes!

Education extends past attorneys to include secretaries, contractors, and anyone employed by the firm. Any weak link in the chain of cybersecurity can cause a breach of data. To ensure the awareness is comprehensive and complete, firms must require new lawyers, and established attorneys, to complete data privacy and data security training programs. [302]The American Bar Association now offers a series on cybersecurity which comes with its own certification at the end of the program. [303]Alternatively, small firms can look for free resources and videos online. [304]

67

[*95] b. Security Software

Security software is the biggest protection a small law firm can have. The *2015 Solo and Small Firm Technology Guide* recommends internet security suites that give much more functionality at a lower price than individual software recommendations. [305]The book does not recommend targeted protection, such as antivirus software, claiming it is not sufficient to keep systems protected. [306]Enterprise versions of security software suites can be the best protection against an individual hackers tools: spam, viruses, malware. [307]The tools in these suites can include firewall management and secure file sharing (like Workshare). Most software, like Kaspersky, even includes functions to change settings on laptops once an employee leaves with the device. [308]

Security provisions should also be implemented on mobile devices such as phones. At minimum, phones should have a password, and have some means of remotely wiping the data. [309]The FTC requires devices, even cellphones, be secured. [310]Both iPhone and Android have either built in software or apps to wipe and track these devices. It is also recommended firms use more secure phones, like Android and Blackberry, which are more capable of using security **[*96]** software. [311]

68

c. Notification Laws

Small firms must also ensure their compliance with state data notification laws. Forty-seven states have laws governing data breach notification. [312]Despite state data breach notification laws, Model Rule 1.4 mandates attorneys tell their clients if data is breached. [313]The only question to a small firm therefore is, when must I notify my client? Small firms can easily research their state standard and adopt policies accordingly.

Firms could also add the notification law to their education provisions. A firm should be aware of not only the timeline in which notifications must be made, but also the level of data breach necessary in order to justify notification. If a small firm has clients across multiple jurisdictions, a firm can more easily adopt the most restrictive standards. [314]

69

d. Encryption

Encryption is probably the most inexpensive and effective form of protecting client data. Encryption is a formula that transforms computer data anyone can read, into data only those with a password can read. [315]Both Windows and Mac computers with enterprise licenses have built in encryption software. Once **[*97]** implemented, hardware like laptops, hard drives, USB drives, and more can only be accessed by those that know the password. Encryption can also be used to protect data in motion, such as over wired or wireless networks, including the internet. [316]Firms can encrypt their phone lines too, making conversations with their clients secure and confidential.

Encryption is so powerful that the FBI Director James Comey has been lobbying to gain "backdoor" access to encrypted data. [317]However, encryption is only as effective as the password used, so firms should push for training their employees on effective password management. Encryption is also available on phones. The *2015 Solo and Small Firm Technology Guide* recommends using Android or Blackberry because their software architecture is much more conducive to encryption mechanisms. [318]Smartphones are always with us and susceptible to being lost or stolen. Encryption is one effective mechanism to protect the history of phone calls made to that client, and the search on LexisNexis for that case.

If client data is compromised, encryption provides a "safe harbor" in some states. [319]If a state has "safe harbor" laws, then so long as the data is encrypted, law firms do not have to notify their clients of the breach. However, Model Rule 1.4 requires notification regardless.

70

[*98] e. Bring Your Own Device Policies

For a small firm, bring your own device can be both a blessing and a risk. Bringing your own device allows attorneys to use software and services their firm does not provide for them. However, an attorney can expose a firm to a host of new malware and viruses when they bring their device within Wi-Fi signal of the firm. [320]But attorneys want and sometimes need to take their materials home or away from the office. [321]

Bring your own device policies need to be managed to account for the added risk. Current standards resoundingly ask for "reasonable measures" for a firm, accounting for the risk of the material. The risk phones pose to personal information is great, but is it enough to outweigh the benefits? The best provision would be to eliminate bring your own device provisions and present attorneys with dedicated devices for work. Such a provision would allow a firm to implement specific security measures on all devices, and ensure compliance with policy. However, this can be a major expense for small firms.

71

f. Written Plan & Policy

If a firm does not have a plan for security breaches, or a written policy on computer use, get one. A written policy for a small firm can provide guidance to attorneys and prevent potential problems. A written policy can be more effectively taught to other attorneys in the firm. It also provides a standard to which everyone is held accountable. If one employee creates a cybersecurity threat for breaking the written policy, they may be reprimanded accordingly. A plan also requires the firm to consider potential threats proactively, bringing cybersecurity to the forefront of a firm's mind. A written plan further helps a firm comply with FTC standard of addressing security vulnerabilities.

g. Small Firms: A Conclusion

Small firms are in a tough spot when it comes to **[*99]** cybersecurity. They face the same threats as a large firm, but with less resources. Solutions like encryption, written plans and policies, managing bring your own device provisions, notification and training are simple, and mostly inexpensive solutions to a firm's needs. This starting point for small firms provides nearly comprehensive protection from threats and liability.

72

How medium sized law firms can protect themselves from cyber attacks

73

Medium firms ought to hire information technology expertise and purchase cybersecurity insurance. Combined, these provisions will offer tailored advice on how to better secure client information and protect a law firm's bottom line from liability.

a. Information Technology Expertise

Medium firms should seek out information technology expertise. Law firms are already mining for cybersecurity lateral hires, in the wake of clients seeking better security protection. [322]Whether a firm chooses to hire, contract, or consult an information technology specialist, the expertise they can offer is incredible. More than this paper can offer, an expert in the field can make specific assessments of risks and solutions for any size firm. However, these services usually **[*100]** come at a high rate, and may be precluded from some medium firms.

b. Cybersecurity Insurance

Cybersecurity insurance is an effective but expensive solution for medium-size law firms. As law firms become increasingly liable for data breaches, owning cybersecurity insurance would protect against losses from the inevitable cyber incidents, including business interruption, network damage, and data breaches. [323]For now, cybersecurity insurance can be obtained--in some cases--with few requirements, perfect for a medium firm. Currently, premiums and limits are determined using traditional point-in-time risk assessments. [324]However, this method may change as insurance companies strengthen their minimum cybersecurity standards. [325]

74

How large law firms can protect themselves from cyber attacks

75

Large firms have many more employees and data to secure. They are expected to not only monitor the security of all of their attorneys in many departments, but also store their data effectively. No wonder the "likelihood of data breach increased to 50% among companies with more than $ 4 billion dollars in revenue." [326]Large firms, however, have more resources for cybersecurity solutions. They can afford premium security suites, professional technology training, and can spend more time planning for the inevitable cyber breach. In total, law firms are spending as much as 1.9% of their gross annual revenues--seven million dollars per year--on information security. [327]

[*101] For large firms, the previous sections look very similar but with more effective means. Large firms can conduct training with professionals, video recordings, or the firm's IT specialist. Notice can be a difficult subject for large firms, as they must reach clients in multiple jurisdictions with different laws. In those cases, where jurisdiction is across multiple states or countries, large firms should follow the lead of large corporations and comply with the most stringent standards.

Large firms may go above and beyond small and medium firm provisions to keep secure their clients' data. The term "may" is used here willingly, as no amount of policy or statute can demand the provisions below. Rather, the provisions described are more ethical obligations, or good practice, than mere compliance with broad standards. However, clients may expect--or demand--the following provisions.

76

a. Cybersecurity Alliance

Large law firms have the new opportunity to join a cybersecurity alliance. A cybersecurity alliance is a venue for firms, banks, and other companies to share information about cyber threats and develop defenses and best practices to prevent them. [328]In fact, 82% of businesses with high performing security practices collaborate with other businesses to grow their cybersecurity protection. [329]Corporations in the Midwest have created their own alliance called the Midwest Cyber Security Alliance (MCSA). [330]It recently held a micro-conference **[*102]** in Saint Louis, Missouri, bringing in IT experts, attorneys, government agents, and more to collaborate on this tough subject. [331]There is also the National Cyber Security Alliance (NCSA), composed of many businesses from across the nation. [332]Security alliance membership is a great venue for large firms to meet, share, and learn best practices to defeat cyber threats.

Recent legislation aims to aid such alliances. The Cybersecurity Information Sharing Act (CISA), passed by the U.S. Senate in October of 2015, allows the government to share its security indicators in these discussions. [333]The legislation also allows big companies to share cyber threat data with their competitors without antitrust litigation. [334]

77

b. Full Reports

Large firms should explore paying information technology specialists to proactively prevent attacks. Wall Street banks already pay information technology specialists to dig into shadowy online forums to see how their brand and information is abused. [335]For instance, banks hire companies like Black Cube that search the "deep web" for data on their client. [336]The company essentially befriends potential enemies before a cyberattack. [337]Black Cube then shares the **[*103]** cyber attackers' intent, information, and means with their client. [338]Sometimes, once Black Cube has enough information, they turn in the hacker to the authorities. [339]Another company, Fox-IT, was even able to get the source code to a new malware program from similar work and share it with their clients. [340]For a law firm, paying for the information available on the deep web can provide a full picture of cybersecurity and proactively prevent future attacks.

78

c. Standardized Certification & Frameworks

Large firms could also seek out standardized certification and frameworks. In recent years, several standardized certifications have been passed that allow a firm to stand out from its competitors. As clients continue to recognize the importance of cybersecurity at their law firm, these certifications are a great way to prove a firm is meeting a certain standard of security. However, these certifications require time, money, and expertise not usually available for small or medium firms. The below is a framework and certification to consider.

The National Institute of Standards and Technology for Cybersecurity Framework (NIST) is one type of standardization framework that is possible for law firms. [341]The NIST framework is great for large firms that are still making big strides to secure their information. The framework divides cybersecurity protection into four tiers. The tiers can be used to identify where a business is in terms of security, and where they can go. [342]Major provisions of the standard **[*104]** include assessing major threats, continuously monitoring those threats, and implementing certain provisions to correct each threat. An added benefit of the NIST framework is it highly encourages collaboration between other participants. As a result, a firm can learn from others who have attained the certification.

The International Organization for Standardization (ISO) has its own set of standards called ISO 27001 Certification. As described above, Shook, Hardy, & Bacon recently attained this certification. [343]The certification is designed to assess risks for businesses and divert assets to protect the riskiest information. Once the requirements of the certification are complete, companies are entitled to market their firm as ISO 27001 Certified.

Because the certificates above push security provisions based on risk assessment, the reasonable measures standard can likely be met by firms who attain these certifications.

79

d. Lobby for Standards and Laws

Large law firms should also lobby for more effective and efficient laws to combat cyber attackers and educate lawyers. The government's statutory laws need the input of law firms in order to better address cybercrimes and set a comprehensive standard for the legal community. One statutory solution to combat cyber criminals is to increase the punishment for cybercrimes. The EU in 2013 assigned harsher penalties to cybercriminals. [344]The US sought to do the same with the Deter Cyber Theft Act of 2014. [345]However, harsher penalties for cybercrimes have done little to deter cyber criminals. [346]Large firms should instead lobby for a more effective means to discourage cyber criminals. [347]Large firms should lobby for solutions that give law **[*105]** enforcement more tools to find and arrest criminals, including funding to promote such programs. [348]Large firms could also educate lawmakers on the legal industry's relationship to cybersecurity, as the American Bar Association Cybersecurity Handbook recommends. [349]Being a part of the conversation on these laws can ensure that firms can take reasonable measures to secure their data. [350]

80

Large firms can also lobby the American Bar Association House of Delegates to pass more strict and uniform standards for attorneys. The ABA House of Delegates did attempt to make more concrete cybersecurity requirements on August 12, 2014. [351]However, the passed resolution is unabashedly vague. The original legislation required all law firms, big and small, to come up with cybersecurity standards that complied with national and international requirements. [352]The legislation was largely rejected by small firms. [353]However, such a requirement could do wonders for the legal industry. **[*106]** For small and medium firms, understanding how "reasonable measures" would apply to the data they store can be difficult. Large firms should take the lead on establishing requirements that are much clearer for firms of all sizes. Although more defined requirements for law firms may push some firms to spend more resources on security, it is a necessary evil. One firm that has ineffective security might create a bad reputation for the legal profession as a whole. For example, if a client presents very sensitive information to their attorneys, and that information is leaked due to weak cybersecurity, that client may reconsider disclosing sensitive information to any firm in the future. It is important that clients feel protected at any law firm to some extent. Therefore, the culture of attorney client privilege is a motivator for large firms to lobby these changes.

81

FEATURE: HOW CYBER RISK CAN AFFECT YOUR LAW FIRM

October, 2021

Reporter
58 AZ Attorney 20 *

Length: 3858 words

Author: BY Jennifer Moreno

JENNIFER MORENO, CISA, is an REDW Information Technology & Cybersecurity Consultant. She joined the IT consulting group in 2015 after serving in REDW's internal IT group for 13 years. She has acquired substantial experience in IT audits, IT risk assessments, cybersecurity assessments, policies and procedure development, security awareness training, and other IT consulting services for tribal and public governmental and not-for-profit entities. She is responsible for IT Risk Assessment and regulatory compliance for the firm and helps develop strategic and tactical IT plans. As a member of REDW's Business Continuity Planning Committee, she also assisted with creation of REDW's Information Technology Governance Council.

82

Level-Up From Prevention to Resilience

Because data storage in general has shifted from being on premise to being in the cloud, network perimeters are no longer easily contained in your firm's local network or local internet connection. In short, IT departments no longer have physical control over the network to prevent bad things from happening. In simpler times, a firewall used to be the digital gateway managed and monitored by the IT department, but now firewalls include each of the valued team members who operate in your firm. It's time to improve elasticity in your cybersecurity practices--we call this *cybersecurity resilience*. Here are key components to start implementing or improving upon at your firm:

IT Governance

IT governance directs the IT function and strategy, and assists with ensuring executive leadership is tuned into operations and verifying alignment with overall strategic, business and risk-management objectives.

Ultimately, executive leadership will be held responsible for data breaches and ransomware attacks, which is why it is imperative that there is a strong IT governance presence within your firm.

83

IT Policies & Procedures

Develop formal IT-approved security policies and procedures to provide guidance for essential processes. IT security policies should provide the basis for an information security program, establish the direction for processes and controls, and manage user responsibilities in their acceptable use of firm technology. Once the firm's IT policies and procedures have been documented and approved by management, remember to review them annually to ensure processes are accurately adopted and communicated to firm staff.

Technology Strategy

As technology risks grow, preventive systems need to advance. Firewalls, intrusion detection and intrusion preventions systems, GEO IP filtering, endpoint protection, advance threat protection, secure remote access, mobile device management, and multi-factor authentication are all security implementations law firms should consider to optimize security protocols and create best practices.

- Patch and update systems regularly to close the gap on software vulnerabilities.
- Research and improve data backup technology and cloud backup alternatives. Practices like these have played an integral role with data recovery after an incident.
- Conduct regular internal and external IT audits, as well as technology risk assessments, to help your firm recognize and close technology gaps and assist in prioritizing risk.

84

Implementing a cyber security awareness program

85

Security Education & Awareness

One of the single most important steps firms should be taking to mitigate cyber risk is to educate employees. For years, IT prevention systems have been in place to thwart off bad actors. However, a recent article from Hacker News [2]cites IBM that 95 percent of all breaches were related to human error. Cybercriminals these days are seeking to create opportunity in hacking *people*, not necessarily just systems. In your firm, the absence of a robust and continuous employee cybersecurity awareness training program leaves the door wide open for cybercriminals.

Implementing a Cybersecurity Awareness Education Program

- Ensure firm leadership understands the risks of an uneducated workforce.
- Create a program that incorporates onboarding, proactive and reactive training for all employees, contractors and temporary workers.
- Establish reporting percentages to help management measure training performance throughout the year; set a risk indicator percentage goal to keep your firm on track.
- Require training throughout the year, keeping employees engaged and up to date with new threat schemes.
- Include interactive training modules with follow-up questions to keep employees engaged.
- Phish all team members on a regular basis to provide teachable moments; implement remedial training for employees who underperform.
- Establish an approved policy and plan early on how your firm will handle noncompliance with meaningful sanctions; ensure zero tolerance for those who fail to comply with remedial programs.

86

Monitoring & Assessment

The average time from a data breach to detection is roughly six months, and almost all breaches are detected by someone else--often the FBI. Assessing existing monitoring systems and conducting routine penetration testing and network vulnerability scans will help identify network gaps and mitigate cyber risks. Proactive monitoring of the network with real-time alerting will assist your IT team in detecting rogue network activity. Implementing Security Information and Event Management (SIEM) provides realtime visibility and analysis across information security systems.

Data Classification & Retention

Know where your clients' sensitive and critical data is located on the network. Create a data classification and retention policy to identify the different types of data your firm maintains and how long each type of data should be retained. Conduct an inventory of all data and establish classification levels such as *confidential, sensitive, public*, etc. Once this data has been mapped out, ensure employees have been provided the appropriate data-access permissions to mitigate the risk of an unintentional or intentional data breach.

87

Incident Response

Time is of the essence when responding to a cyber incident. It's essential that your firm have a documented incident-response plan that details best practices so your IT and **[*24]** incident-response teams can effectively and efficiently respond to a variety of identified cyber incidents. Your incident-response plan should:

- Establish the owner of the plan and define ownership duties
- Have a cybersecurity incident response plan (CSIRP) team that will define a clear mission, roles and responsibilities
- Include training and testing requirements for the CSIRP team to ensure plan familiarity and contribution to the response and recovery process
- Identify multiple types of incidents and classify the severity of each
- Implement tools for incident detection and analysis to determine plan initiation scenarios
- Define a communication process to manage end user expectations in an incident
- Include steps for containment, eradication and recovery to ensure you are able to stop the attack, remove it from the environment, and get team members back in action
- Ensure there is an investigative process that will include evidence-handling procedures
- Ensure expectation for a post-incident event or report to document event

88

Business Continuity & Recovery

When the COVID-19 pandemic first hit, many businesses didn't have a business continuity plan to pivot from office environment to a work-from-home environment, which negatively affected operations. This case can also be made if an organization experiences a ransomware attack. Should a data disaster be declared, best practices for business continuity and recovery must have been previously established to assist law firms in identifying effective and efficient recovery processes. Having a documented and tested disaster-recovery plan, with detailed recovery-point objectives (RPOs) and recovery-time objectives (RTOs), is vital for ransomware recovery or any other cyber risk that affects systems and data.

Insurance Coverage

Obtain cyber-liability insurance coverage to help protect your firm should there be a cybersecurity incident. Ensure you're working with a well-versed broker or consider having an independent third party review the policy to ensure necessary coverage. Look for complimentary pre-breach services or postbreach services such as a "data breach coach" should you need guidance through the process. As many policies are unique, understand what your firm policy covers and carefully review the policy exclusions and limitations.

Key coverages to look for in a cyberliability policy are business interruption, computer fraud, social engineering, privacy and security liability, and ransomware. With the increase in cybercrime, insurance companies are taking into account best practices that their clients (or potential clients) have implemented. Not having best practices (such as a formal security awareness training program, an incident-response plan and multi-factor authentication) could make your firm an undesirable risk when seeking to obtain insurance coverage.

89

Third-Party or Managed Service Providers

We are repeatedly reminded of cybersecurity incidents happening to organizations through a third party (Target, Home Depot) due to the absence of IT vendor management. Unfortunately, this happens all too often to small and medium businesses who trust their third-party vendors (or managed service providers) to have robust security processes and controls in place. Law firms should be managing and vetting their vendors to mitigate cyber risk by requesting to review service provider SOC2 audit reports, confirmation of cyber-liability insurance, and by reviewing service contracts.

It's also imperative that your firm actively monitor *any* vendor access to the network, and that you ensure strong security controls are implemented over appropriate vendor access to prevent them (unintentional or intentional) opportunity into your firm's sensitive data.

Creating a culture for cybersecurity awareness is essential for law firms to prevent cybercriminal access to highly sensitive client data, such as Social Security numbers, medical information, health insurance information and even biometric data. Leadership must take an active role in cybersecurity and understand that responsibility no longer belongs solely to the IT department. Incorporating proactive and resilient cybersecurity protocols in your firm's practices will help create a strong and vibrant cybersecurity posture and help your firm stay on top of ever-evolving cyber risks.

90

Federal government resources

91

92

SMALL BUSINESS TIP CARD

America thrives with small businesses in society. There are numerous opportunities for small businesses to fill needed niches within the industry. However, many small businesses may not have all the resources they need to have a strong cybersecurity posture. By implementing simple cybersecurity practices throughout the organizations, small business can safeguard their information and data for increased profits.

93

SIMPLE TIPS

1. Make sure all of your organization's computers are equipped with antivirus software and antispyware. This software should be updated regularly.
2. Secure your Internet connection by using a firewall, encrypt information, and hide your Wi- Fi network.
3. Establish security practices and policies to protect sensitive information.
4. Educate employees about cyber threats and how to protect your organization's data. Hold employees accountable to the Internet security policies and procedures.
5. Require employees to use strong passwords and to change them often.
6. Invest in data loss protection software, use encryption technologies to protect data in transit, and use two-factor authentication where possible.
7. Protect all pages on your public-facing websites, not just the checkout and sign-up pages.

94

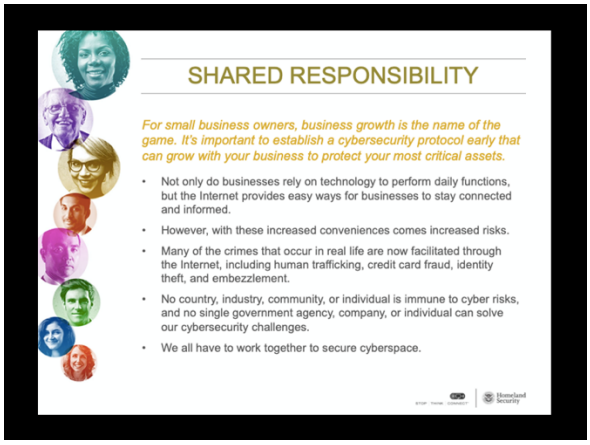
IF YOU'VE BEEN COMPROMISED

- Inform local law enforcement or the state attorney general as appropriate.
- Report stolen finances or identities and other cyber crimes to the Internet Crime Complaint Center at www.ic3.gov.
- Report fraud to the Federal Trade Commission at www.onguardonline.gov/file-complaint.
- Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov.

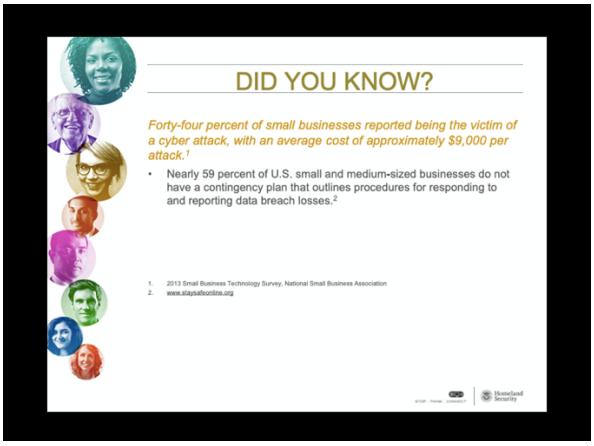
95

96

97



98

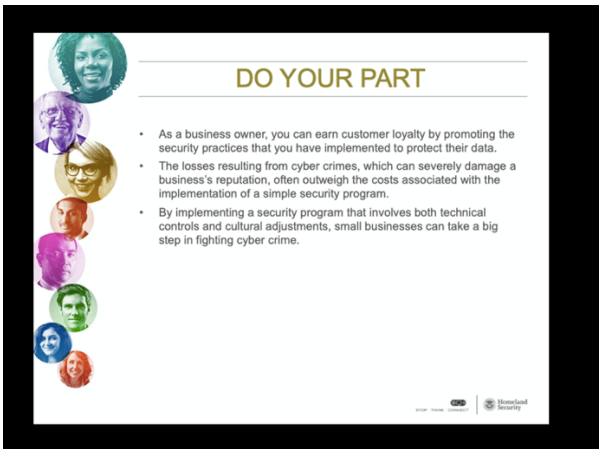


99

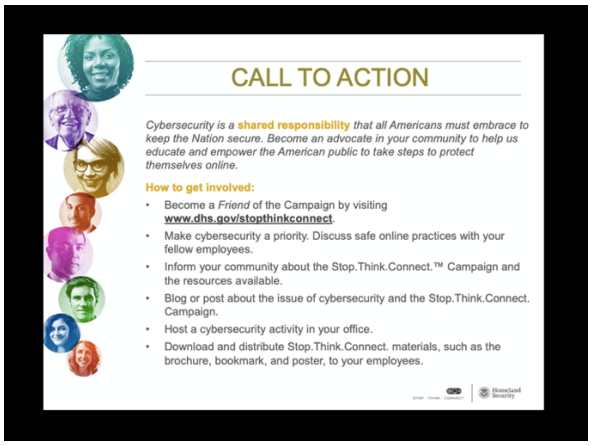
100

101

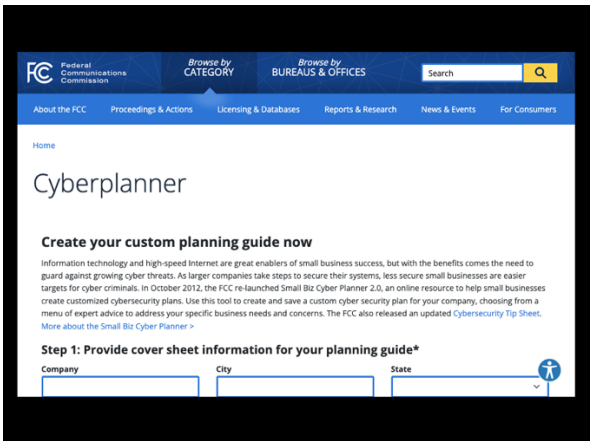
102



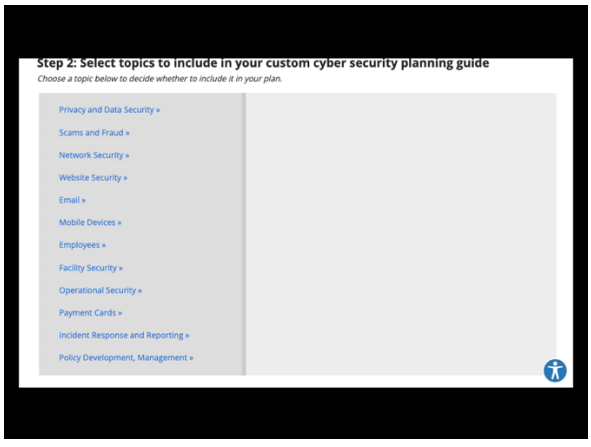
103



104



105



106

Some helpful links

Cyber security for small business

https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses

Cyberplanner

https://www.fcc.gov/sites/default/files/cyberplanner.pdf

CISA Cybersecurity Awareness Program Small Business Resources

https://www.cisa.gov/resources-tools/resources/cisa-cybersecurity-awareness-program-small-business-resources

107

ROLAND GARY JONES, ESQ.
TEL: (347)862-9254
FAX: (212) 202-4416
E-MAIL: rgj@rolandjones.com
www.rolandjones.com

Mr. Jones has practiced bankruptcy law for over two decades. His primary focus is representing corporate defendants in preference and fraudulent conveyance litigation. He has developed a national client base and has also represented corporate clients based in Europe and the Far East.

Mr. Jones is the author of "Bankruptcy Preference Clawbacks in Plain English: Why They Exist. How to Defend Yourself," currently available on Amazon.com., as well as the producer of over 50 videos on Preference and Fraudulent Conveyance available on Youtube. Mr. Jones is also the founder of a new bankruptcy litigation blog: www.onebowlinggreen.com.

Clerkships: 1989-1990 Chief U.S. Bankruptcy Judge Conrad B. Duberstein of the Eastern District of New York; 1990-1991 U.S. Bankruptcy Judge Cecilia H. Goetz of the Eastern District of New York from 1990 to 1991

Bar Admissions: New York State Bar Admission – 1990; United States District Court Southern District of New York –1991; United States District Court Eastern District of New York –1991