LEGAL REVOLUTIONary
Journal of the Digital Economy

Protecting the confidentiality of M&A deals at the law firm side

Practical cybersecurity measures to apply today

Alexander Sverdlov | Founder | Atlant Security

29 May 2020

LR 2020, Pages 164 to 167 (overall 4 pages)

A law firm can build its reputation based on what kind of clients and deals it can serve and the bigger the clients, the higher are the risks with the deals they bring on the table. When you sit with your client on one side of the table and on the other side you have the buyer/seller of a company and their law firm and financial advisors, you definitely do not want to lose the leverage you have (or the leverage you helped your client find) to win. 1

I. Mergers and Acquisitions can fail before even getting to the negotiations table due to a micro-misconfiguration in your IT systems

One sure way to lose that leverage and cause major harm to your clients is if you fail in preserve the confidentiality of crucial details of the deal through a cybersecurity breach. 2

Your client company's valuation depends on how well your firm preserves any confidential details and documents before and many times even after the deal is signed. 3

It is also your responsibility to let your client know that confidentiality depends on their bankers, attorneys, financial advisors, their own employees, their family, their board, and shareholders who are aware of the pending deal. Attorneys are just one link in the chain, but a very important one. 4

Trusting the confidentiality of any critical details to a confidentiality and a non-disclosure agreement is not practical, because people make mistakes and systems get hacked. There are things in your control and in your responsibility which you must take care of besides the legal documentation. 5

II. Preventing breaches by security awareness and security culture

Your employees are the first line of defence in protecting any information entering your firm, starting with the office managers, paralegals, lawyers and ending with managing partners and their family – building the culture of awareness of how easy you can lose control of crucial information can make the difference between being safe and being the firm that leaked client data before a deal. 6

Security awareness trainings are often brushed off to HR to organize – this is a major mistake. HR has no idea what amount of information your team needs, who needs a different kind of training from the others and most importantly, they do not have an idea of what kind of threats this security awareness should protect against. It is important to trust your cybersecurity consultant in the assessment of how aware your team is of potential cybersecurity risk and then the selection of the right kind of training to give them. 7

"Don't click on links in suspicious emails" does not work. Attackers nowadays have had decades in experience in producing just the right content for just the right audience so that the emails, sms messages and instant messages will always sound and look legitimate. They may even hack a trusted partner of your law firm in order to send an email from a legitimate address with malicious content – how will your team recognize that scenario, if you send them to a low-quality, generic security awareness session? 8

Awareness is just a small portion of the larger goal of building a culture of protecting information in the firm in general. 9

This culture should also include regular drills, or exercise, aiming to test your employees in their vigilance and alertness, because people grow less alert over time or when you repeat the same 'be careful' message over and over again. 10

III. Technical measures you can take to ensure a breach does not happen in your systems

You have several very common points of failure, most of which have to do with communication or access control. 11

Communication:

1. Email – your most critical asset and the easiest to breach

The underground market has prices ranging from $100 to an average of $1000 to breach a corporate email account. Usually the hackers guarantee a successful hack within 24- 12

48 hours of getting the order. Considering many M&A deals are in the range of hundreds of millions of U.S. dollars it is easy to see how small a price someone could pay to get into your firm's email systems. Enforcing 2-factor authentication before anyone can log in to their email on the web is an absolute must.

2. Instant Messaging – do you use WhatsApp or similar apps to discuss deal details with your clients?

Please avoid that practice – in fact, it is a good idea to forbid it to anyone under your control or whom you are advising. Only use secure, encrypted instant messaging apps and only when there is no way to share confidential information over a more secure channel (in person or on paper). Always prefer tamper-proof sealed paper envelopes to any other form of communication for highly critical documents (such as the Confidential Marketing Memorandum which usually contains the client company strategic plans, assets value, customer demographics and much more). Remember: it is possible that a phone on any side could get stolen or lost and all the information in it – leaked to the press or your client's competition. 13

3. Your DMS (Document Management System) or your cloud file sharing / storage solution

Your DMS (Document Management System) or your cloud file sharing / storage solution, even your on premise, internal document storage and sharing system could be compromised. Take extra care to ensure they are monitored for suspicious activities and at the very least have very tight access controls over who uses them and take especially great care of the highly confidential documents of your clients stored there – with a clear 'need to know' rule of granting access. There is one important detail here: your IT administrators usually have full access to everything. What if a hacker gains control over an IT admin account? Have you taken this risk into account? Have you planned and implemented any measures to control or even prevent that risk? 14

It helps if you try to think from the hackers' point of view. If they get an order to get into your systems and steal information on a deal, how would they approach the task? 15

- Is hacking your Wi-Fi (a 10-minute task for a hacker, usually) enough to grant someone access to confidential data from the coffee shop across the street?
- Is it easy to fool your users into revealing their passwords?
- Is it easy to hack into your email servers?

- How do you control the password complexity of your systems? Can someone select a password such as 'password' or P@ssw0rd123? Do you audit your systems for frequently used, easy-to-guess passwords which pass the complexity requirements but are still easy to guess, like the one above? It is important to point out that if you outsource your IT to a 3rd party provider as most law firms do, they tend to do a very poor job in securing your systems – their specialty is fixing computers and selling ready-made solutions, even when it comes to security – they package and sell firewalls, antivirus applications, but rarely have the understanding of how modern attackers operate and how breaches happen in order to prevent them. If you can afford it, hire an outside security consultant to assess your practices and systems, to assess the work your IT provider has been doing over the years and suggest critically important improvements before your firm becomes one of the breached ones (and according to ABA every year more than 20% of all law firms get hacked, compounding the number to over 80% in 10 years).