Anatomy of a Data Breach

by Sharon D. Nelson, Esq. and John W. Simek

"I could have evaded the FBI a lot longer if I had been able to control my passion for hacking."

- Kevin Mitnick (the first hacker to make the FBI's 10 Most Wanted List)

Introduction

Hacking can indeed be a passion, proving that you can outfox governments and big league corporations. The thrill of the chase can be addictive – and the addiction is fueled by the monies to be made.

Breaches come in many variants, far too many to cover in a single article. But there is a general flow to a breach. Since we make a living investigating breaches and remediating the vulnerabilities that caused them, let us take you on an anatomical tour of a typical breach, highlighting some of the common elements.

To make the reading more fun, we have offered up "quotes" from the players typically involved in a breach. Many are taken from real-life incidents.

Hackers: "Let's plan our attack."

Whether there are massive attacks of automated bots looking for vulnerabilities and exploiting them or spearphishing attacks (tailoring a phishing email to a specific target), there is planning. When state sponsored hackers from China attack governmental facilities in the U.S., the planning is intense – and highly coordinated. These hackers are often working in government buildings. Other hackers, primarily cybercriminals, belong to loosely affiliated groups – they are often working together in the ether, not in a physical location.

Many cybercriminals are looking for a known vulnerability to exploit – this was the case with the WannaCry ransomware, which succeeded so well because Windows 7 users hadn't timely patched their operating system.

If you want to, you can go on the Dark Web and buy a vulnerability. It is not quite as simple as an Amazon 1-Click purchase, but it's not hard either. Some hackers will pay big money for a "zero-day" piece of malware (one that has never been used and therefore no specific defenses exist against it). Some will pony up a lot of cash (or cybercurrency) for a previously undisclosed vulnerability, again with a high probability of success.

Do they want to attack through the weak security of Internet of Things devices? Do they want to exploit all the entities, including law firms, which have moved to Office 365 without properly securing it? There are many decisions to make. They involve targets, attack surfaces, tools, objectives, dates, methodologies, etc.

If they are crafting phishing e-mails, the more sophisticated hackers will hire native English speakers to help them – that means that poor grammar and wrong forms will not give them away.

Like the old-time grifters used to say, there's no con without a plan. And part of the plan is not getting caught, right? So you use a sleight of hand. If you're Russian and you want to hide the source of the attack, you do some technical magic and now it looks like the attack came from China. Hackers are all about smoke and mirrors.

Hackers: "3-2-1 – FIRE!"

When it is time to push the button, the hackers involved are usually pretty intense in watching their attack proliferate across the globe – or if they are spearphishing, they are on high alert watching for a response to their bogus or spoofed e-mail. Or they are waiting for an unthinking employee to click on an attachment (containing malware) or click on a link to a website (containing malware).

Some results are fast, some less so. But you can be sure the watchers are riveted, monitoring the results of their handiwork. The truly sophisticated don't even watch. They have automated systems that notify them automatically when a target has been breached.

Hackers: "We're inside. Let's pwn everything we can!"

If the point of the breach is to purloin data, the hackers will try to use their malware to move laterally across your network and "pwn" ('hackerspeak' for 'own') everything they can. Imagine the value of data in a mergers and acquisition law firm. You could sell the data to others or use it yourself to get rich on the stock market. State-sponsored hackers can give their countries a competitive advantage against the U.S. Economic espionage is more and more common.

The longer a hacker is inside the network, the more the hacker learns about the network itself and its users. That knowledge can be a springboard for figuring ways to compromise more user accounts and gain access to more data. One primary objective is to keep the attack hidden.

We haven't made a lot of progress in discovering data breaches. According to the *2018 Ponemon/IBM Cost of a Data Breach Study*, it still takes an average of more than six months to discover a data breach – and the mean time to contain the breach is 69 days. This gives hackers a lot of time to gather your data.

Law firm managing partner: "Oh crap, we've been breached."

'Crap' may or may not be the exact word choice, but we have heard many such utterances. They are generally made in a nervous (sometimes hysterical) voice – and the stress of dealing with a data breach is immediate – and runs throughout the investigation and remediation. The stress is worse if knowledge of the breach becomes public.

If the law firm has an Incident Response Plan, it is the first resource for those within the firm in charge of dealing with the breach. They begin picking up the phone to call the regional office of the FBI, their insurance company, their data breach lawyer, their digital forensics company, their bank, and the list goes on. All 50 states now have data breach notification laws, so those will be carefully read to determine if a report (or reports) must be filed and when.

Rarely, if ever, does a law firm notify clients at this juncture. In most breaches, it is not immediately known what data may have been compromised – and there is natural reluctance to tell clients anything until the investigation is well underway. The exception is when the breach goes public – and then there is little choice but to talk to clients.

Law firm receptionist: "The FBI agents are here."

There is something about the arrival of the FBI agents that unnerves those delegated to meet with them. In our own experience, the agents are polite but somewhat humorless. Understandably, from their point of view, it is a Joe Friday "Just the facts ma'am" kind of meeting.

If it makes you feel better (at least slightly), the agents do not arrive in marked vehicles and they are not wearing the emblazoned FBI jackets. They are also not loose-lipped – you will not find an account of their meeting with you leaked to the press or elsewhere. They are in the business of keeping things confidential.

But be forewarned, it is not their place to do the actual investigation and remediation of the breach – that job belongs to private digital forensics investigators. This seems to disappoint some law firm leaders, who hope that the FBI can "fix the problem." The FBI agents are there to gather data. This is how the government gathers facts which may help everyone, for instance by sharing information about hacking methods, tools, groups, etc. through such vehicles as the FBI's Infragard program.

If there are national security implications to the breach, the FBI may bring in colleagues from other agencies, notably the Department of Homeland Security. At that point, they may go beyond information gathering and take actions – but that is the exception rather than the rule.

Digital forensics investigator: "Yeah, we know how they got in. You pretty much sent them an engraved 'hack me' invitation."

OK, the investigators will probably be more diplomatic. But between themselves, this is often the conclusion they reach – that the client's security was sloppy. It is exceedingly rare for qualified, highly certified digital forensics investigators not to find the cause of the breach, though it may take time. As noted above, the average time to contain breaches is 69 days – 69 days of long, hard, excruciatingly detailed work, with every step carefully recorded.

Progress reports will be given regularly to law firm management. Once it is known how the hackers got in, you will be informed. Remediation steps and their costs will be presented for approval. Given that there has been a breach, there's usually not a lot of deliberating about spending the monies.

Typically, breaches are traced to a long list of possible causes (the engraved 'hack me' invitation), including users clicking on a link in or attachment to an email, sharing of log-in credentials, reusing of passwords, weak passwords, failure to update/patch software, lost or stolen devices, privilege misuse, insecure websites, malicious insiders, social engineering, etc. But at the end of the day, there is generally some kind of malware which must be rooted out of the network – and this process can be time-consuming and complicated.

Longer term recommendations usually include employee training, phishing tests (with consequences for multiple failures, up to and including termination), regular security assessments and penetration testing, in which the security company acts as though it were an attacker.

Law firm insurance company: "We don't cover 'stupid'."

The cyberinsurance world remains the Wild, Wild West. With a notable absence of historical data to guide the industry, even Warren Buffet, CEO of insurer Berkshire Hathaway, is skeptical. He said in May of 2018, "Cyber is uncharted territory. It's going to get worse, not better . . . There's a very material risk

which didn't exist 10 or 15 years ago and will be much more intense as the years go along." He went on to say, "We don't want to be a pioneer on this ... I think anybody that tells you now they think they know in some actuarial way either what [the] general experience is like in the future, or what the worst case can be, is kidding themselves." We could not concur more.

Buffet's views are reflected in more and more cyberinsurance policies, which now often include requirements for security audits and also include language about conforming to industry cybersecurity standards, The case we refer to above because it became known in the press as the "We don't cover stupid" case is *Columbia Casualty Co. v. Cottage Health System*. There are now more cases in the judicial system where insurers are saying the insured did not take the reasonable security steps required by the policy. We certainly know a lot of law firms whose cybersecurity practices wouldn't stand up to some of these new insurance requirements of "best practices" or "industry standards."

Law firm client (whose data was compromised); "We need to reevaluate our association with your firm."

The sound of clients beating a path to the law firm exit door is a scary thought but in light of all the law firm data breaches that have become public, we know that more and more clients are not taking even long-term relationships with law firms as a continued certainty where cybersecurity is lacking.

Ten years ago, only a handful of clients seemed deadly serious about demanding that their law firms demonstrate that they were focusing – and spending money - on cybersecurity. That has markedly changed. Now clients are demanding that law firms fill out security questionnaires and sometimes demanding a third-party audit which certifies that any critical vulnerabilities found have been remediated.

In 2017, the Association of Corporate Counsel upped the ante when it released *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information*. The gauntlet was effectively thrown down, identifying the standards outside counsel are expected to meet with a hint of "or else."

Law firm management meeting: "Anyone think we need to spend more money on cybersecurity NOW?"

From our foxhole, there is a bit of "We told you so" in seeing law firms, given a well-thought cybersecurity proposal, reject the proposal and then suffer a breach because of the very vulnerabilities that were addressed by the proposal. From our colleagues in the cybersecurity industry, we understand that this happens all the time. It is frustrating. Much of the time it has to do with spending money (hence the subhead above) or simply a wrong-headed belief that "it can't happen here."

On a regular basis, you probably see CLEs advertised focusing on how to get cybersecurity buy-in from law firm management. Data breaches have a marvelous way of getting law firm ostriches to remove their heads from the sand. With perfect clarity of vision, they now see that cybersecurity is an integral part of any law firm's risk management planning. And they do tend to crowbar open their wallets, especially when their clients or their insurance company require various reassurances.

Final thoughts

At the end of the day, hackers want your data or your money and sometimes both. Their motivations are not complex. You may remember the movie “Bonnie and Clyde” and the scene where Clyde announces to strangers, “We rob banks!” Simple, to the point, and said with pride. Hackers, who are also criminals, are generally equally enthused about their work.

When you are up against an expert hacker with a wide array of hacking tools and sufficient funding, you don’t have much of a chance. Your best defense is being prepared and making cybersecurity a priority. The hacking community is gunning for you – of that, you can be quite sure.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com