IT Audits: Is Your Firm Ready?

How to Effectively Manage Increasing Client Security Requirements

by Christopher Perrotta & William Pate, Innovative Computing Systems, Inc.

Long gone are the days of basic security precautions like simply installing antivirus software and having a dedicated IT team. Today is the era of two-factor authentication, longer and stronger passwords, clean desk policies, mobile device management, network encryption and partnering with the right vendor to perform security scans and audits to keep your law firm ahead of hackers and malicious actors. Defense-in-depth is an old but increasingly relevant concept and strategy.

Gone, too, are the days of naively assuming our confidential data is secure. Increasingly, clients, stakeholders, regulators and others are demanding proof that firms are actively protecting the personally identifiable information (PII) to which they have access, and this evidence is being demanded both before and after security incidents. In fact, such audits are likely to occur for many firms without a cyberattack being the trigger.

Law firms must have the positions and processes in place to handle security incidents with urgency, accuracy and completeness. This white paper gives legal professionals the background on security audits, the rise of ransomware, and what to do before, during and after an attack.

The Rise of Security Audits

Security audits of law firms' information infrastructure and practices are becoming more commonplace as more businesses deal with clients' PII and other forms of sensitive information. Companies must continue to take the necessary steps to safeguard themselves not only from hackers but also lawyers, judges and juries. Major recent lawsuits have been filed over poor handling of data, and some of these have been incredibly expensive.

Notable Breach Settlements

Facebook – $5 billion
Anthem – $115 million
Target – $28.5 million
Home Depot – $19.5 million

Source: https://www.classaction.com/data-breach/lawsuit/

IT Audits: Is Your Firm Ready?

Vendors are beginning to offer security scanning, especially as law firms continue to invest in protecting both themselves and their clients, representatives and vendors.

Regardless of industry, if a business has a partner or a vendor, it can expect an information security audit, if only because someone wants to ensure the firm is meeting the security requirements covered in most agreements.

Security Audits: Why They're Important

Security audits scan your network, provide you a list of vulnerabilities, ensure your firm is following established security policies, and that it has incident response and business continuity plans in place. The importance of such plans is hard to overstate as these are the processes and responsiveness documents that need to be referenced to keep your company alive after a cyberattack.

Many companies reach out to their IT team or managed service provider (MSP) to perform a security audit. Why is this important for your firm? Sixty-three percent of all small and medium-size companies go out of business after a major cyberattack. Being prepared by having proper procedures in place for employees to follow before, during and after an incident is what determines whether your business survives.

Even if your data makes it, what about your clients' data? What about your firm's reputation? These are all impacted, and your ability to identify, resolve and recover from an attack is what ensures you stay in business.

How Ransomware Works

Ransomware is intentionally malicious, requiring little human involvement to implement and hold your data ransom for a large sum of money with no guarantee of data restoration.

In many ransomware cases, malicious actors will focus on leveraging weak passwords and common accounts from the outside. They constantly bombard a system for commonly used passwords. A firm must have a solid password policy, two-factor authentication and specific rules for outside access to its network to block most of these intrusion attempts. Once the program gains access to a firm's system, it runs a simple executable that encrypts the machine's drives with a nearly unbreakable level of encryption. It then infects every other device on the network by searching local devices before forcing owners to pay a ransom in bitcoins for a chance to restore their files. Even if one pays the ransom, however, file restoration still is not guaranteed.

Approximately 8% of paid ransomware ransoms lead to no resolution. Further, by paying to restore its files, the firm ends up funding criminals and other hostile actors who will only be emboldened to continue their profitable ventures by infecting others and holding them hostage as well.

Cost of Ransomware Attacks on Municipalities

- Texas – $2.5 million ransom, $12 million business impact
- Baltimore, Maryland – $76,000 ransom, $18.2 million business impact
- Atlanta, Georgia – $51,000 ransom, $17 million business impact
- Lake City, Florida – $500,000 ransom (paid), undisclosed business impact
- Riviera Beach, Florida – $600,000 ransom (paid), $941,000 on new network infrastructure, undisclosed business impact.

The Realization

You attempt to log in to your system and cannot. *What's broken this time?* you think, as you call your IT person for help. They log in and notice the ransomware. *Oh no…*

This is how many law firms realize they have been compromised. This is the basis of a standard cyberattack today. You might think, *I paid the ransom, so things are good, right?* Wrong. You have had a stranger inside your network with likely unfettered access to your server and, therefore, all your data.

What kind of data did they look at? What data did they take? These questions are answered by having a designated individual and an incident response plan to handle this. This is the next step, the pivot to security and acknowledging processes to be ready before, during and after an incident.

Before an Attack

Are you ready for a cyberattack before it happens? Having policies in place, running frequent security and network scans and maintaining updates on all machines – from the printer down the hall all the way to the servers in the cloud – are key to reducing your firm's exposure and increasing the difficulty of improperly accessing your data and avoiding an attack.

A hardened network will do more to protect your firm by frustrating and discouraging hackers, and it is far less expensive and time-consuming than recovering from a successful breach.

Once an attacker has been given access and data has left your network or been locked down due to ransomware, it is too late. Stopping an attack from occurring is much less onerous than the time, energy and money spent on recovering lost and damaged data and facing the legal consequences of such an event.

During an Attack

If your firm is under attack right now, you should have a business continuity plan to guide your firm through escalating the issue appropriately. Additionally, your firm should have individually prepared processes for various attacks based on severity and type as each of these scenarios requires a different way of handling the issue.

Is this a cyberattack? Is this a compromised account utilizing ransomware? Is this leaked information from a malicious employee? In the case of compromised hardware, what data was compromised? Were software and PII compromised? What about compromised infrastructure? What information was accessed? These are all questions your company needs to know as part of its incident response plan so that the right decisions are made.

After the Attack

The moments after an attack are when the survival of a compromised business is determined. If your firm planned and prepared for the inevitability of an attack, confusion, time-to-remediation and overall business impact will be reduced.

How to Get Buy-In from Your Firm IT Committee/Managing Partner

Being prepared for cybersecurity incidents helps in dealing with them when they happen. Make sure your law firm's IT team supports how important security is to the ongoing success of the business. If 63% of SMBs go out of business after a major cyberattack, your firm should be defending itself at all costs. That means investing in the security planning, infrastructure, documentation, processes and people needed to ensure business continuity.

It is your responsibility as a firm to build and maintain valid trust with your clients. If you do, they will keep coming back for more of your services and help your company's ongoing growth. Make sure the same delicate care you provide your clients is also given to their data.

It is never too early to be prepared for issues that may arise from a cyberattack. In fact, it's better to be prepared. Being aware and ready to deal with cybersecurity failures makes them less scary and easier to respond to. The experts at Innovative Computing Systems can help your firm take steps to effectively manage increasing client security requirements.

Protect your firm's data, your clients' data and your reputation today. Contact an Innovative Computing Systems Account Executive at 1-800-541-0540 or sales@innovativecomp.com.

About Innovative Computing Systems, Inc.
Innovative Computing Systems is the first-choice partner of law firms, legal departments and professional services organizations looking to define or improve a comprehensive IT strategy; implement, integrate and support best-in-class legal and horizontal technologies; enhance cybersecurity and leverage the power of cloud computing.