ACCELLIS
TECHNOLOGY GROUP

Practical Guide to Cybersecurity For the Small Firm

Table of Contents

Introduction

Every day we hear about a new hack or breach happening somewhere. Our own privacy and security are under constant assault. If you are reading this, there is a good chance you have already had a security incident. If you have not, the statistics say it is only a matter of time.

Cutting through all the clutter and noise about organizations, big and small, falling victim to hacking, or ransomware is becoming increasingly difficult – even downright confusing. Where to begin has become a challenge.

"Is my firewall enough?"

"Does my anti-virus keep me safe?"

"How do I even know if I have been hacked?"

The security industry produces a plethora of volumes of education, training, hardware and software, professional services, and other elements that feed into building a comprehensive cybersecurity program – often called the *cybersecurity domains*.

While it requires commitment, developing a practical guide to cybersecurity for your firm need not be complicated or even all that expensive. In this report, we will outline some tools, services, and tips that even the smallest practice can use to prevent or mitigate an attack.

But first, let us start with what has happened to most law firms – you have been breached. Not in the past tense, but in fact you are likely – at this very moment – harboring a criminal actor or malicious software within your network.

Besides the standard "zero-day" attacks we have all heard of, ransomware attacks can leverage software that may have been downloaded days, weeks, or even months ago. To address this situation, you must develop an Incident Response Plan.

SONY PLAYSTATION 2011

DISCLOSURE

77 MILLION ACCOUNTS

Hackers seeking financial, PII, and other information breached 77 million accounts

TYPE

Theft + Hactivism

Sony: “We discovered that the intruders had planted a file on one of our Sony Online Entertainment servers named ‘Anonymous’ with the words ‘We are Legion.’”

VECTOR

For under $10,000, Sony could have purchased vulnerability scanning which would have detected the common coding flaw (SQL injection) before a breach occurred.

FALLOUT

Stocks fell by $7.58(24%) between April 2, 2011 and June 20, 2011. In all, the attack cost Sony between $100 and $170 million and PlayStation online services suffered a staggering 23-day outage.

Incident Response Plan (IRP)

Your clients no longer expect you to prevent a breach. If Target, Sony, Equifax, and Mossack Fonseca (Panama Papers) cannot completely protect data, how can you?

The breach itself is no longer the biggest risk companies face – it is the backlash from clients and customers if they find out that you had no plan to recover when the cyber event happens. In this section, we help you to craft a basic IRP to keep yourself and the firm's reputation protected.

Incident vs Breach

There is a nuanced yet important distinction between a *cyber incident*, where information is *exposed*, and a *breach*, where information is *disclosed*.

In the first case, information was simply exposed while in the second, information was likely copied from your network. The distinction is important from a response standpoint.

For example, client data taken from your network (disclosed) would require client notification while ransomware (exposed) may not.

Your Incident Response Plan will leverage this distinction by connecting the different breaches to the potential exposure of information and required remediation efforts.

As not all cybersecurity incidents are created equal, the plans to deal with them need to be equally unique based on the risks they represent. In addition, the type of hack or breach that occurs can tell you a lot about what the perpetrators intend, which informs you of your next steps in a response.

Types of Breaches

Breaches can be classified into three types: theft (money or information), ransom, and access. Others may be a concern, such as hacktivism, but for this document, we will focus on those breaches more common to small and midsized firms.

1. Theft

Breaches with an intention of theft typically come into the network through advanced social engineering attacks (e.g., a spear phishing attack targeting a legal assistant or attorney working in mergers and acquisitions). These attacks steal information or trick one of your employees into divulging bank account information for what is really a fraudulent wire transfer. These breaches are often difficult to uncover or identify until it is too late.

2. Ransomware

Your data is held hostage for payment by encrypting it so you cannot use it. Unlike a theft breach, ransomware attacks generally occur through larger, less targeted campaigns like spam email blasts. This type of attack is one of the biggest threats to the legal and financial service industry. Perpetrators cast a wide net to induce people to click a link or open an attachment that carries the code to encrypt data. With ransomware, the perpetrator executing the attack works to reveal the breach so you know who and how to pay.

3. Beachhead

The third breach intends to simply use your firm's network as a launching point into another organization or to co-opt it as part of a larger attack on another organization. Beachhead breaches, while unnerving, tend to be less damaging.

Less Common Attack Vectors

Firms should know of all the attack vectors and various methods employed to steal data and cause harm to an organization. The IRP should identify the assets at risk and primary targets in an organization. For example:

Attack Vector / Method	Assets at Risk	Primary Targets
Crimeware + Ransomware	All data	All employees
Cyber Espionage	Equipment and data	All employees
Denial of Service	Website, web services	All employees
Man-in-the-Middle	All data	All employees
Insider + Privilege Misuse	Financial, M&A, HR data, IP	Exploiting rights & privileges
Physical Theft or Loss	Hardware assets, databases	Server C://; firm laptops
Web Application attack	Cloud-CRM & QuickBooks Online	Partners, Admins, & Controller

MOSSACK FONESCA

PANAMA PAPERS 2016

DISCLOSURE

11.5 MILLION RECORDS

An epic leak of more than 11.5 million financial and legal records exposing a system of offshore companies accused of corruption and wrongdoing.

TYPE

Hacktivism

Hacker John Doe: "[I leaked the documents] simply because I understood enough about their contents to realize the scale of the injustices they described."

VECTOR

An "astonishing disregard for security" including failure to update both its Outlook Web Access login since 2009 and its client login portal since 2013.

FALLOUT

The political repercussions were stunning: a four-day war (Azerbaijan and Armenia), mass protest worldwide, resignation of Iceland's Prime Minister. and even the recent murder of Panama Papers journalist Daphne Caruana Galizia.The firm shuttered dozens of offices.

Responding to a Cyber Incident

Now that we have a better understanding of what we are responding to, the key elements of your IRP must include:

Responsible Individuals

The IRP should list the individuals responsible for containing the breach (typically IT), responsible for recovering data lost (also typically IT), and who notifies clients, partners, and the authorities (typically a partner).

Detection, Response, and Timing

Based on the breach, each responsible person should know what the necessary tasks are to contain the damage. Priorities include:

1. Verification of breach type

Verification starts with determining type of breach, stolen devices, information leaks, and stolen or modified documents. Information breaches are often discovered when sensitive information has been leaked. Ransomware is discovered as documents become inaccessible due to encryption.

2. Initiation of mitigation plan

Take all affected equipment offline immediately. Closely monitor all entry and exit points, especially those involved in the breach. Put clean machines online in place of infected ones.

3. Initiate communications plan

All information should be documented well before a breach occurs. It is advisable to keep this information off the regular network in the event of malicious encryption. Relative to the breach type and depth, notify:

- Management and employees
- Local and federal authorities
- Legal counsel
- Data forensics team
- Clients

4. Secure network, social media, and web credentials

If the data breach involved personal information improperly posted on your website, immediately remove it. Be aware that internet search engines store, or “cache,” information for a period of time. You can contact the search engines to ensure that they do not archive information posted in error. In addition, update credentials and passwords of authorized users. If a hacker stole credentials, your system will remain vulnerable until you change credentials, even if you have removed the hacker’s tools.

5. Secure forensics

Generally, turn no machines off until the forensic experts arrive – instead, disconnect the machine from the network. Specialized forensics teams will take it from here.

6. Recovery procedures

Identifying the breach
Identify the type of breach and where it may have occurred

Determine breach produced data loss
Review logs and check the integrity of your file server, document management system, and practice management system.

Information recovery
Execute recovery procedures by restoring data from backups.

Documentation
Document at each step: how the breach occurred, how it was discovered, the damages, and the recovery processes employed.

Now that we have a business response plan, let us talk about some basic measures you can implement to reduce the chances of another breach.

EQUIFAX

2017

DISCLOSURE

145 MILLION RECORDS

Hackers seeking financial, PII, and other information accessed records on more than 145 million Americans.

TYPE

Theft + Cyber Espionage

USA Today: “The reason the hackers wanted the data is likely financial... or it could have been the work of a country looking for data to use for intelligence purposes."

VECTOR

Apache Struts software had vulnerabilities detected in March. Patches became available shortly thereafter. Equifax failed to update and patch regularly to protect themselves.

FALLOUT

The IRS suspended a recently rewarded $7.2 million contract. According to Chicago attorney Jay Edelson, "if done right" the class-action lawsuits will see Equifax pay more than $1 billion in damages.

Building Your Cybersecurity Program

A comprehensive cybersecurity program is effective when awareness and understanding are baked into the firm culture and the first step is knowing that your law firm is the steward of valuable information. Understanding that your data can be turned into "gold" for someone else or that your network can be leveraged in an attack on another organization, or worse, on one of your own clients, is paramount to comprehending the severity of the situation. Once you know what you stand to lose, building a defensive posture around it becomes less complicated.

Policies & Procedures

Implement policies and procedures

While some clients and industries may require specific and detailed written information security policies and procedures, every law firm should have a few basic, but very important ones.

1. Passwords: the U.S. government's new NIST security framework, recently updated and published this year, spells out new guidelines on how to approach passwords. Passwords remain the single most common method of authenticating into your firm's resources. The new guidelines suggest passwords should be more complex and unique, but frequent password changes are no longer recommended.

2. Disaster Recovery: even the most secure organization will be compromised and data loss will occur. Having a good backup and disaster recovery plan is paramount to successful recovery and a critical element to that plan must be testing the restoration of files and whole systems regularly, not just during an actual security event.

3. Vendor Security Program: your firm is focused on providing legal services to your clients. You rely on a variety of vendors to provide business services to keep your firm operational, from payroll to paper delivery and from copy machine repair to IT support, a lot of people have access into your inner-workings. Establishing a policy and implementing accompanying procedures to verify access reduces the chance of exposing your firm from the inside-out; just ask Target. Carefully define requirements to help vet vendors and require all vendors to pass annual audits to ensure they are making every reasonable effort to protect their information and access into your firm.

Take-aways: Passwords should be at least 12 characters in length and include at least one uppercase letter, one number, and one special character to increase difficulty in a dictionary attack; incorporating a Barracuda Backup Device or similar Backup and Disaster Recovery (BDR) solution will allow files to be recovered quickly and reliably if files are damaged, deleted, or ransomed from the system.

Limit user access to only necessary data and applications

The "principle of least privileged access" is a well-known and commonly established security concept which limits access to line-of-business applications, firm data, and other client files to just those who need it. This significantly diminishes the chances of someone accessing something they should not access in the first place, and limits what can be stolen from any single individual at the firm.

1. Firm operations: software and data used in the day-to-day operations of the firm, such as human resources files and financial data, usually offer additional security controls within the application. Bank account number and personally identifiable information (PII) are frequently sought after. If the firm is using something like QuickBooks to manage the finances, be sure to password protect the files through the application. Personnel records can be saved in a directory on the file server or within a document management system that allows granular permissions and control.

2. Practice and case management software: provides granular permissions and access control to client files and matters, export capabilities, financial information, documents, and more. Locking attorneys to only their clients reduces the chance of data theft and unauthorized access, while mitigating how widespread the theft will be in cases of breach.

3. Document and content management software: allows managed grouped access reducing the chances of a security incident. Both practice and document management software provide excellent detective controls using audit logs and trails, which makes it much easier to get an accurate picture of what was accessed, by whom, and when.

Take-aways: Configure your accounting, practice management, and document software for "least privileged access"; lock down files on your network using network permissions.

Establish "safety-stops" for financial transactions

Increasingly, attempts are being made by cyber criminals to trick you into processing payments and wire transfers. These are usually done through social engineering and spear phishing attacks. Inserting checks and balances into the processing of payments and other financial transactions will mitigate loss.

1. Guidelines – establish guidelines that encourage looking at potentially unusual behavior, such as new transfer requests, an unusual number of recipients, or different business or contact information than you have on record. Be aware of typos and misused gender pronouns.

2. Security features – most banks offer a host of optional security features to protect against fraudulent transactions. Speak with your primary contact at the bank to make sure your firm is utilizing the safety features available.

3. Place a call – to the point of contact receiving the funds. This simple step could have saved a California law firm $500,000. It takes a few minutes.

Take-aways: Create procedures to verify transactions; work with your financial institutions to make sure all safeguards are in place.

Secure Client Communications

Communicating with clients, vendors, and partners creates the opportunity for data exposure. In order to mitigate this risk, firms need to implement controls on email, stored data, phones, etc. Two elements are at particular risk.

1. Email encryption – implementing secure email encryption will go miles towards minimizing your risk of data exposure or disclosure. Once setup, only recipients can access information in emails and attachments.

2. Secure document sharing – many firms engage in the practice of emailing files to coworkers, vendors, and clients. This introduces the possibility of data exposure or disclosure. It also hurts the performance of email systems which much load unnecessarily large mailboxes.

Take-aways: Citrix ShareFile *is one of the top file sharing utilities. It gives firms the ability to send files, audit them, revoke access, and more.* Barracuda Essentials *offers agentless email encryption allowing firms to send encrypted emails without requiring complicated key management.*

Technical Defenses

Insight and visibility

Logging and monitoring the activity within your network and services provides critical insight into how files and services are being accessed. This information, when compared with an activity baseline, illuminates potentially malicious activity.

Alerts can bring a possible breach to your attention so the IRP can be put into action quickly. Timing is critical; the longer a breach goes unchecked, the costlier it tends to be.

While there are several types of logging and monitoring, it can generally be lumped into two groups:

1. Active Directory and network monitoring: utilizes logging systems built into most server and workstation operating systems to record account access to files and track logons and logouts. If you notice a copy machine account being used to log into a secretary's computer and accessing client files at 2 AM in the morning, you might have a problem.

2. Malicious activity monitoring: aims to track account usage and other activity for malicious and abnormal behavior. By establishing baseline activity, malicious activity monitoring can easily alert you if someone is using your network login from Ukraine, while you're in your office in the United States. By monitoring *behavior* rather than *signature*, many systems respond faster.

Take-aways: Enable Active Directory logging or deploy another logging solution, such as Snort*; subscribe to a malicious activity monitoring service similar* Rapid 7's insightIDR*.*

Block the traffic that does not belong

One of the simpler actions your firm can take to help protect your assets is to block traffic that does not belong on the network. If your firm is not doing business in China, firewalls and other services can be configured to block network traffic to and from that country.

1. Geo-blocking: is a configuration, often made on a firewall, that blocks activity from IP addresses originating from specific geographic locations. While it raises the chance of a complication (e.g., you are traveling abroad), it is an extremely effective measure. One recent hack into a law firm in New York siphoned valuable client data back to servers in China. Geo-blocking IP addresses in China while making exceptions for known good IP addresses would have considerably minimized the damage to that law firm.

2. DNS protection services: are similar to Geo-blocking. Specific domain names are blocked from transmitting data to and from your network. DNS protection services differ from Geo-blocking in that the service dynamically blocks known bad domain names. As new malicious servers come online and become known to the service, DNS protection services kick in to actively block access to them.

Take-aways: Configure Geo-blocking on your firm's firewall; subscribe to a DNS protection services, such as Cisco's OpenDNS Umbrella.

Ensure Disaster Recovery

Disaster recovery is a critical element to organizational security. If a firm has backups but no disaster recovery, they are only half secure. In the event of a virus or ransomware, backups can mitigate the situation entirely.

1. Offsite Disaster Recovery – establish a secure offsite backup through replication to either a cloud provider, a server or storage appliance in another geographic location, or through offsite rotation of external media.

2. Testing – a critical and often neglected part of the backup and disaster recovery process is backup verification; the firm needs to periodically verify, by way of actually restoring the data, the authenticity and efficacy of data backups.

3. Extended backup rotation – firms should seek to establish a Grandfather-Father-Son backup rotation. This is a schema for backups that establishes the thresholds for incremental, daily, weekly, monthly, quarterly, and annual backups. Alternatives to GFS are Tower of Hanoi or First in-First out.

Take-aways: most backup and disaster recovery solutions now offer data center replication or device-to-device replication, meaning firms can begin to ditch external hard drives and tape drive systems; test backups in a secure sandbox rather than on production systems; establish a backup schema consistent with retention needs, compliance requirements, and budget.

Encrypt your data and devices

Data and devices left unencrypted present a significant vulnerability that can expose your firm's data. Mobility offers lots of benefits but using unencrypted devices in public spaces makes for an easy target. Moreover, when it comes to sharing information, attorney-client privilege is sacrosanct. Despite this, the primary method of sharing files with clients remains email and attachments, which is by default transmitted in unencrypted form.

1. Securely sharing with your clients: using services and features like Citrix's ShareFile or Microsoft's OneDrive allows you to safely communicate and share important files through encrypted channels. Files can be monitored, given expiry, and require passwords.

2. Encrypting data at rest: all data stored by your firm must be encrypted. This is particularly important to do with your backups. Since your backups represent such a rich aggregation of everything important to your firm, encrypting backups is critical to ensure every reasonable step was taken to protect your client data.

3. Encrypt devices: all smart phones have built-in methods for encrypting the device. Most versions of Windows, Mac OSX, and even Linux also have built-in methods to encrypt data. Disk encryption helps safe guard portable devices, making the data unusable unless the correct key is entered to decrypt the data. This helps mitigate the ramification of devices physically stolen.

Take-aways: Purchase files sharing services, such as Citrix's ShareFile or Microsoft's OneDrive (which is built into Office 365); use mobile device management to ensure all devices are encrypted; turn on BitLocker (Windows) or FileVault (macOS) to encrypt workstations and laptops.

Secure remote access

As mobility has become such a large part of the business landscape, challenges to making sure remote access to your data remains secure have also grown in complexity. By enabling a few key technologies, you can connect to your firm with a greater sense of confidence.

1. Secure Connections: implementing a secure VPN or similar technology allows you to get to your firm data more safely. This is particularly important with the growing prevalence of free Wi-Fi hotspots in the public and at hotels. A secure VPN creates an encrypted channel for you to directly access firm resources while using public connections. Also, use enterprise remote access where possible (e.g., Microsoft RDP rather than ShowMyPC).

2. Multi-factor authentication: a key element of many of the recent large hacks has been the theft of user databases, including usernames and passwords. Cyber criminals often use passwords as part of a brute force attack on networks around the world. Deploying multi-factor authentication, whereby users must use more than one factor to login, such as something you know (password), something you are (fingerprint), or something you have (security token), counterbalances the threat of single factors that can be easily compromised.

Take-aways: Setup and configure VPN or RDP access to firm resources; configure your firewall to force multi-factor authentication when connecting from outside the office or purchase and deploy a multi-factor authentication solution, such as Yubico or RSA's SecurID.

Education & Governance

Human resources and employee governance

Onboarding and offboarding of employees presents an excellent opportunity to instill a sense of awareness and understanding of cybersecurity threats, as well as ensuring access controls are appropriate and evaluated frequently.

1. Employee onboarding: review and certify that new employees understand the technology, policies, and procedures that help protect the firm. Validate that proper security access is given to new users so they can access only what they must in order to get their job done.

2. Employee offboarding: make sure permissions and access to firm data and services are appropriately removed from user accounts and that all firm assets have been returned. Deactivate inactive users and devices in Active Directory, and initiate mobile device wipe.

Take-aways: Develop employee onboarding and offboarding checklists to ensure proper training and access for new employees and that access is removed for departing personnel.

Offer formal and regular education

Whether it is the technology, the policies, or the procedures, educating and training firm members remains one of the most important things your firm should undertake. Security technology has steadily improved but people remain the biggest Achilles' heel. Raising awareness of the persistent threat and improving understanding of the technology and procedures in which the firm has invested is among the top ways of decreasing a firm's risk exposure.

1. Validating the training: providing a "pop quiz" for training validation is a great way to keep security awareness at the forefront of users' minds. Cybercrime can happen at any moment and user readiness must be up to the task. Properly executed, a "pop quiz" will challenge an employee's ability to recognize potentially malicious elements through a fake email. Many cybersecurity training services off customizable templates to make emails look legitimate, replete with web links and attachments. Activity in the email is recorded so your firm can narrow the training to increase effectiveness.

2. Teachable moments: whether it is through training or looking back on what went wrong following a cybersecurity breach, honest reflection on how to continuously improve and shore up gaps to prevent future incidents will make the firm stronger.

Take-aways: Conduct regular security training to teach users how to spot phishing emails and websites that are malicious in nature. Use products like PhishingBox or KnowBe4 or Barracuda Sentinel to verify end users are following the correct procedure when these items are found.

Accellis Technology Group

Accellis Technology Group is one of the nation's leading providers of IT Consulting & Managed Services for the legal industry. We help law firms of all sizes reduce their day-to-day administrative tasks so they can focus on growing their business. Whether you need quicker access to help desk support, proactive IT management, improved security, or custom software solutions, Accellis can provide the expertise and direction to meet your goals.

This guide was developed by Accellis Technology Group based on years of field experience in the legal industry and is based on the ISO 27001 standards. Accellis Technology Group provides no warranties with respect to the guidance provided by this tool. Businesses should consult a cybersecurity expert before implementing any of the recommendations in this guide.

Additional resources:

- Cybersecurity Policy Handbook
- Law Firm Cyber Security Threat Matrix
- Avoid These Three Common Security Blind Spots
- Penetration Testing vs. Vulnerability Scanning
- Law Firm Cybersecurity: Practical Tips for Protecting Your Data
- Which types of hackers represent the biggest threat to law firms?
- The Biggest Cybersecurity Threat to Law Firms is Not What You Think

Schedule a Free Consultation.

Accellis Technology Group helps simplify and streamline your cybersecurity and compliance efforts. We help you get in front of potential threats by ensuring your systems and policies are up-to-date with the today's latest industry standards and expectations.

Whether it's a security assessment, penetration test, or compliance evaluation – our team of certified security experts can ensure you're on the right track.

Schedule a Consultation

ACCELLIS
TECHNOLOGY GROUP

(216) 662-3200
www.accellis.com/contact-us