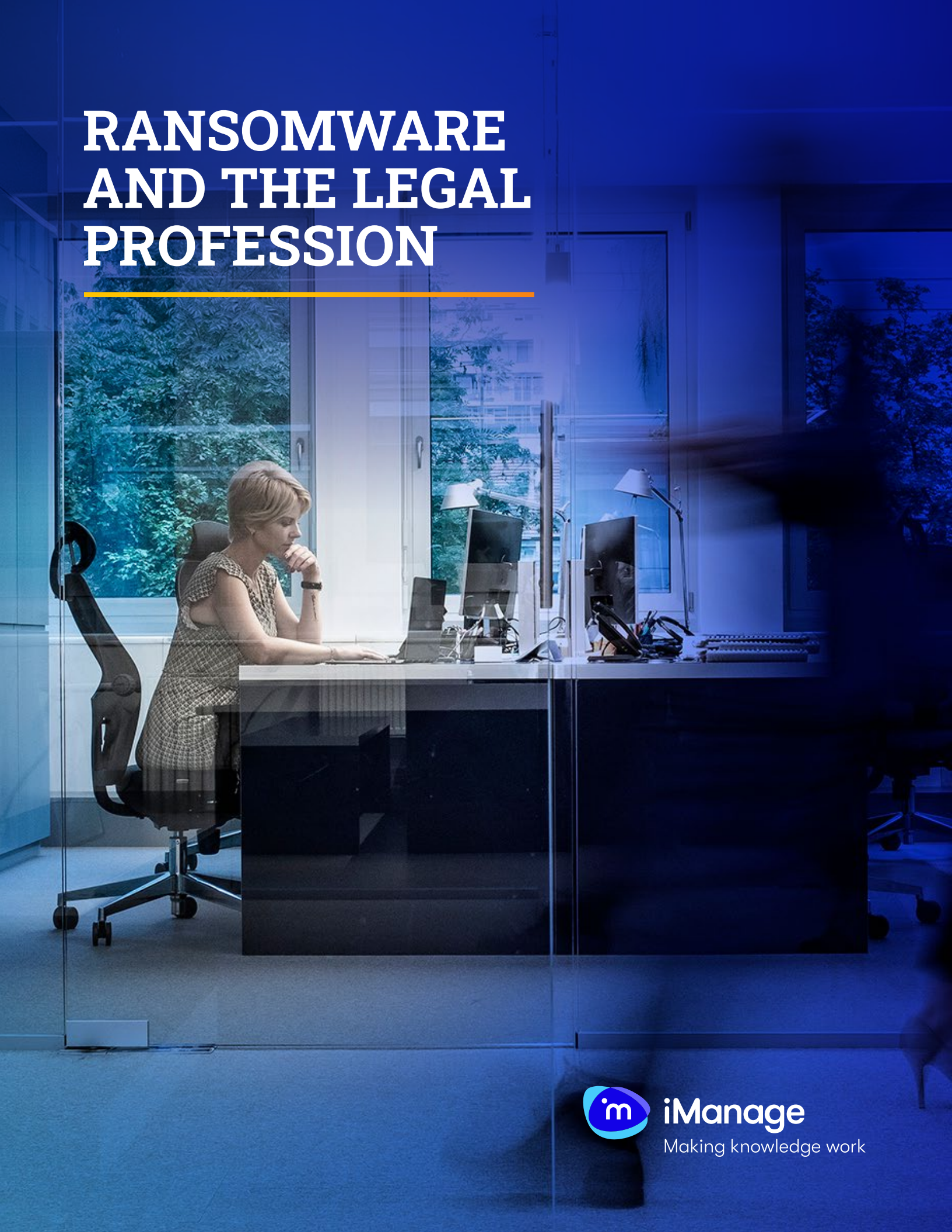
RANSOMWARE AND THE LEGAL PROFESSION



iManage
Making knowledge work

CONTENTS

Ransomware is a growing threat **03**

What is ransomware? 04

Data theft is becoming more prevalent 05

Ransomware as a Service 05

The threat to legal firms **06**

What makes legal firms a particular target? 07

It is getting easier to target legal firms 08

For legal firms, reputation is everything 08

Legal firms must protect themselves from ransomware **10**

iManage Cloud brings ransomware protection 12

How iManage Cloud protects you from ransomware 13

- Administrator controls 13
- Awareness 13
- Backup 13
- Journaling 14
- Network 14
- Patching / vulnerability scanning 14

Conclusion **15**

RANSOMWARE IS AN EVOLVING THREAT AND MORE PREVALENT THAN EVER

Ransomware is a significant threat to today's business world. We hear of new ransomware attacks on an almost daily basis, with the overall number of attacks rising month on month. But what hits the headlines is only the tip of a very large iceberg. Many organizations don't admit publicly to having been the victim of a ransomware attack. The potential for reputational damage is simply too great. Instead they prefer to handle the situation behind the scenes, perhaps extricating themselves without paying up, perhaps meeting the ransomware's demands.

Anonymized surveys which focus on people who work in a corporate technology environment can be much more revealing about the state of ransomware than public admissions of an attack. For its report *The State of Ransomware 2020*, leading cyber security firm Sophos surveyed 5,000 IT managers across 26 countries and found that 51% of organizations were hit by a ransomware attack in the last year.

The UK Government's *Cyber Security Breaches Survey 2021* research found that while phishing remains the most common threat for businesses in the UK, ransomware attacks (grouped with account takeovers, hacking attempts, and other unauthorized access) have a more serious effect. Of businesses that have experienced breaches in the last five years 8% reported temporary loss of access to files or networks, and 6% reported web sites or online services taken down or made slower. The CEO of the UK's National Cyber Security Centre, Lindy Cameron, said in June 2021 that ransomware was the key threat facing the UK.

Travelex

Ransom paid: reported as $2.3 million

Attack happened late 2019 / early 2020. Restoring systems took two weeks, caused reputational damage which could have been a contributory factor in the company's closure in 2020.

Source link

Ransomware is equally prevalent in the US. The Department of Justice has said that around $350 million in ransom was paid to malicious cyber actors in 2020, and that this is an increase of more than 300% on the amount paid out in 2019. The Department of Justice has created a ransomware task force and a web site, stopransomware.gov, to help tackle the problem.

What is ransomware?

Ransomware is a type of malware that is placed surreptitiously inside a computer network. Once it is inside the network, it attempts to encrypt files so that organizations have no access to their data. By blocking access to critical content, it may be able to take web sites down. Removal of the ransomware encryption only comes if a ransom is paid, or if an organization has a data backup and restore functionality that allows it to fully reinstate content to a pre-ransomware state. Ransomware can sit on a system for many weeks before it is triggered, potentially infecting backups and preventing restore being used to annihilate an attack.

Ransomware can send files out of the network to a third party. A subset of the complete data held can then be used by the perpetrators as proof that they have compromising material, or released onto the dark web or other platforms to encourage organizations to pay the ransom in order to stop the release of further data.

If the required ransom is not paid, the stolen data can be published or sold in full, data on the victim's computer network deleted, or the decryption key not provided so that computer systems are no longer accessible.

Ransomware can get into computer systems in a number of ways. The Sophos *The State of Ransomware 2020* research identified a number of methods with their frequency of use:

HOW THE RANSOMWARE GOT INTO THE ORGANIZATION	# INCIDENTS	% INCIDENTS
Via a file download/email with malicious link	741	29%
Via remote attack on server	543	21%
Via email with malicious attachment	401	16%
Misconfigured public cloud instances	233	9%
Via our Remote Desktop Protocol (RDP)	221	9%
Via a supplier who works with our organization	218	9%
Via a USB/removable media device	172	7%
Other	0	0%
Don't know	9	0%
Total	**2538**	**100%**

US Colonial Pipeline

Ransom paid: $4.4 million

Based in Georgia, operates the largest petroleum pipeline in the United States, carrying 45% of the fuel for the East Coast – 2.5 million barrels a day of gasoline, diesel, heating oil, and jet fuel on its 5,500-mile route from Texas to New Jersey.

The Pipeline reported an attack on May 7, 2021. It had to disable the pipeline and take some systems offline. The pipeline remained down for several days.

Source link

Data theft is becoming more prevalent

In its report *Cyber Threats 2020: A Year in Retrospect,* PwC noted a change in the way ransomware actors have operated over the past year. The report notes that they are now more likely to take data from their victims before compromising their systems. This makes sense from the point of view of the perpetrator, as the threat of release or sale can be used to encourage the victim to pay the ransom, as already noted.

Software can sit unnoticed on a system for weeks, slowly leaking information out to bad actors. When they are ready, the bad actors announce that they have acquired data on a public leak site, and require a ransom for its return, threatening release of the data if the ransom is not paid, or perhaps releasing a portion of it as a "taster."

PwC notes that the use of leak sites has "almost certainly achieved its objective of increasing the pressure on victims to pay ransom demands."

Ransomware as a Service

Sophos's *The State of Ransomware 2020* shows that ransomware is no longer just a threat to larger organizations. It found that just under half (47%) of the organizations with 100-1000 employees in its survey were hit by a ransomware attack, while just over half (54%) of the organizations with 1001-5000 employees were hit.

One reason ransomware has proliferated over the last year, and also a reason it is able to target smaller firms, is the growth of Ransomware as a Service (RaaS). Developers build ransomware systems, and then sell a user-configurable service. This has effectively opened up access to ransomware to those who lack the technical skills to build systems from the ground up.

In its report, PwC suggests that the rise of RaaS has helped ransomware grow in scale and scope. Its accessibility to those with less technical knowledge makes it more easily rolled out to smaller organizations.

Brenntag

Ransom paid: reported as $4.4 million (reportedly negotiated down from $7.5 million original demand)

Attack reported May 2021. One part of Chemical distribution company Brenntag's North American division was compromised, 150GB of data was stolen with a public release threat if ransom not paid.

Source link

THE THREAT TO LEGAL FIRMS

Legal firms are a particular target and attacks threaten a firm's reputation

The threat to legal firms

Legal firms may think they are not likely to be victims of ransomware attacks. Larger firms may feel that there are more attractive targets such as national infrastructure or large multinational organizations. Smaller firms may feel they are small enough not to be on the radar of ransomware attackers. Both views might have come about because the kinds of attacks that hit the headlines tend to be of major multinational companies, or large infrastructure. But both views are wrong.

Research from global cyber security firm BlueVoyant found that 100% of law firms analyzed were targeted in attacks by threat actors and 15% of a global sample of law firms showed signs of compromised networks.

BlueVoyant compared its research findings with companies in the 16 sectors defined as critical to securing national infrastructure, resources, and resiliency by the US Department of Homeland Security. BlueVoyant contends that the legal sector should be designated as "sector 17" due to the high-value data law firms contain and their role as arbiters and safe keepers of public trust.

Research by US cyber security provider Purplesec shows that smaller firms are firmly in the sights of ransomware perpetartors, finding that:

- 20% of ransomware victims are small to mid-sized businesses
- 85% of Managed Service Providers report ransomware as a common threat to small to mid-sized businesses
- On average a company experiencing a ransomware attack in 2019 had 645 employees

The US Department of Justice has said that around 75% of all ransomware cases are attacks on small businesses, noting that they often have yet to adequately protect their networks.

In the UK, the *Cyber Security Breaches Survey 2021* reveals that four in ten businesses (39%) and a quarter of charities (26%) reported having cyber security breaches or attacks in the last 12 months.

What makes legal firms a particular target?

For legal firms, as for many others, the publication of stolen information is a significant issue. Even publishing the fact that personal or compromising information about named clients is held by a ransomware agent and could be published at any time is a significant threat a legal firm's reputation.

Campbell Conroy & O'Neil, P.C.

In July 2021 Campbell Conroy & O'Neil, P.C. issued a public notification of a ransomware attack that took place in February 2021.

The firm noted that information relating to individuals was accessed. While not confirming that any specific personal information was accessed, they did confirm that, "information present in the system included certain individuals' names, dates of birth, driver's license numbers / state identification numbers, financial account information, Social Security numbers, passport numbers, payment card information, medical information, health insurance information, biometric data, and/or online account credentials".

Grubman Shire Meiselas & Sacks

Reports said around 756GB of files were put on the dark web related to celebrities like Jennifer Lopez, David Letterman, John Mellencamp, Robert DeNiro, Christina Aguilera, Barbra Streisand, Maria Carey, Andrew Webber, Luther Vandross, Sean Puffy Combs, Rod Stewart, John Mellencamp, Priyanka Chopra, Bruce Springsteen, Elton John, the Kardashian sisters & family, Madonna, Nicki Minaj, Tom Cruise, Dwayne Johnson.

Leaked files include contracts, telephone numbers, email IDs, personal correspondence with the lawyers related to various case files, and non-disclosure agreements made with advertising and modeling firms.

An article at Forbes reports that the initial ransomware demand was $21 million, later doubled to $42 million with publication of over 2 gigabytes of Lady Gaga's contracts and other data on the dark web as proof of compromise. After finding files related to President Donald Trump, the perpetrators doubled the ransomware price and later published 169 emails related to Trump.

Legal firms are increasingly an attractive target for ransomware agents because of the nature of their business:

- Some law firms work for very high profile clients.
- Law firms can hold very sensitive information such as M&A, litigation records, tax details, contracts, forward financial plans, and personal information.
- Law firms have multiple clients. Accessing information about several clients with one attack can deliver more data about more organizations than can be obtained by targeting single firms.

It doesn't matter if a law firm works for top-flight or mid-range clients, they can hold these types of sensitive information, and so there is perceived value to ransomware perpetrators.

It is getting easier to target legal firms

Two factors in particular make legal firms more vulnerable to ransomware today than they have ever been:

- The rise of Ransomware as a Service. When ransomware attacks can be mounted by people without technical expertise, targeting smaller firms which might make smaller payouts but have weaker security, become a viable option for perpetrators.
- The trend for taking information from victim organizations with a view to leaking that information on the dark web makes any organization dealing with sensitive information, or working with people in the public eye a potential target.

For legal firms, reputation is everything

Law firms have a fundamental responsibility to be protect their clients by being good stewards of their privileged information. In order to engage with any client, a law firms needs to certify that they will make every effort to protect their information.

Delivering this can be a challenge as the threat landscape evolves and changes. Many firms can struggle to keep one step ahead. In recent times the Covid-19 pandemic has added a further complication in that it has required first class security for remote workers, and opened up opportunities for bad actors to target firms by revealing security loopholes.

The reputational damage a ransomware attack can cause can bring a law firm to its knees regardless of the firms' size or of whether the ransom is paid. If a legal firm is subject to a ransomware attack, it might decide not to disclose the fact, in the hope that it can mitigate the issue and carry on with business as usual. But this can be a dangerous strategy. Information can leak out in all sorts of ways, and it only takes one person to say something for a rumor to start, and then that rumor can quickly spread.

A law firm that asks itself if the reputational damage caused through trying to keep an attack quiet and failing might be worse than coming clean is asking the wrong question. The right question is to ask how to prevent a ransomware attack from happening in the first place.

LEGAL FIRMS MUST PROTECT THEMSELVES FROM RANSOMWARE

iManage Cloud brings ransomware protection

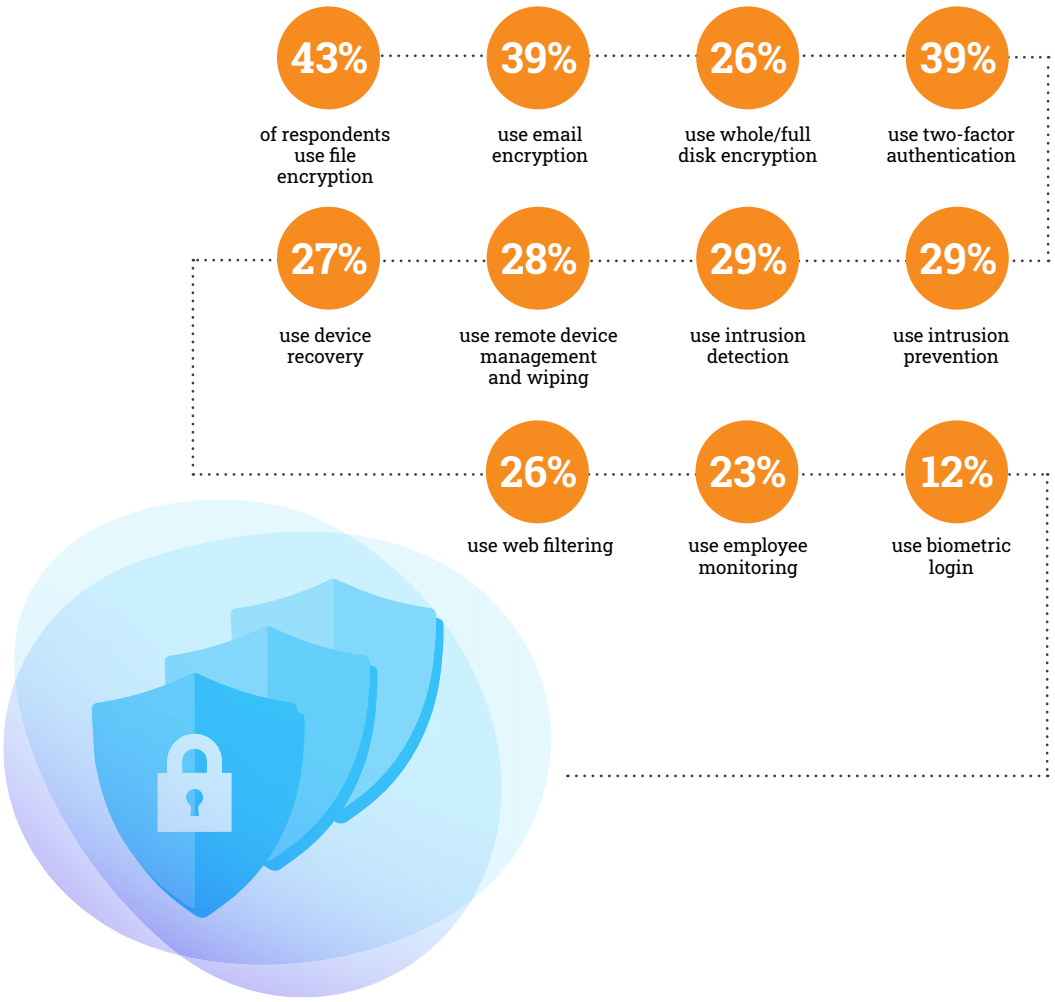
Legal firms must protect themselves from ransomware

For a ransomware attack to succeed several conditions need to be in place:

- An attack vector (the method used such as a compromised email or web site).
- Lack of awareness.
- Lack of patching to keep software up to date or vulnerabilities in the computer network or particular applications.
- Inadequate detection and monitoring capability.
- Inadequate data storage facilities.
- Inadequate data backup and restore facilities.

But legal firms don't always take the necessary steps to ensure protection from ransomware – or from other forms of cyber-attack.

The 2020 American Bar Association Law Technology Report found that use of security tools is patchy. Its survey found:



iManage Cloud brings ransomware protection

iManage Cloud is a cloud-based SaaS platform which provides professional services firms with world-class document management. It enables mid-sized firms to reduce the complexity of their IT management without sacrificing capabilities, and removes the headaches and steep learning curve that can be created by trying to maintain and manage the strongest data security protocols in-house.

When a firm uses iManage Cloud it automatically inherits strong protections against ransomware and other forms of cyber-attack. There are a number of factors at play.

- iManage Cloud is provided to customers only as a web-endpoint that sits outside a legal organization's computer network and has limited interaction with customer services inside the customer firewall. Since it is not attached to the a firm's network, ransomware can't easily jump across.
- Documents are stored in a dedicated data store. There is no facility for any software to run in this data store, so ransomware can't locate them, edit them, or delete them.
- iManage Cloud on Azure offers a foundational customer-specific encryption solution. If ransomware were able to gain access to the files, they would be opaque to the attacker, and could not be used as proof of attack.
- Our customers do not have direct access to the storage layer in the cloud. It is true that compromised credentials could allow bad actors to access documents, but this type of attack is not an entry point for ransomware.
- iManage's Zero Trust Architecture assumes no implicit trust between any two services. Service to service communication must be explicitly granted via IP port and protocol. Consequently it would be very difficult for an attacker to infect our services. If an attacker were able to access services, the hosts do not have internet access so it would be extremely difficult for the attacker to communicate with its command and control systems.

How iManage Cloud protects you from ransomware

Administrator controls

A ransomware attack typically starts with an attempt to compromise an end user or administrator at the company, or a vendor's cloud operations team. iManage Cloud operations personnel are not able to directly connect to the iManage Cloud's services and infrastructure. There is a process in place that breaks the internet connection and requires human intervention:

- The operative goes to a multi-factor VPN system to get access to a jumpbox.
- A device certificate and a one-time PIN is required to connect to the VPN.
- The jumpbox is a restricted device with no internet connection.
- The ability to share drive or transfer files is technically restricted from the administrator device and iManage Cloud infrastructure.

Awareness

Our operations and support staff undergo rigorous and comprehensive training. Examples include:

- Annual awareness training.
- Regular technical incident tabletop exercises.
- An annual "capture the flag" exercise for our engineering teams.

Backup

Ransomware attacks typically try to access every aspect of a system to encrypt data on file servers, any storage media and, importantly, backups. It wants to disable or destroy the backup or recovery mechanism.

- iManage conducts backups of customer data as part of the iManage Cloud service.
- Backups are made hourly and daily. Backups are mirrored across two data centers.
- Backups are kept for 90 days, and are encrypted.

Journaling

A file that has been encrypted by ransomware and uploaded to the iManage Cloud, for example through iManage Drive, can be reverted to a previous version because the journaling feature ensures that a copy is made of every change to a document.

Network

A ransomware attacker needs to be able to communicate status and control back to the attacking server. If the owner of the ransomware wants to extract data to use as part of its claim for a ransom, this needs to be retrieved from the attacked system.

- iManage's Zero Trust Architecture assumes no implicit trust between any two services. Service to service communication must be explicitly granted via IP port and protocol. iManage Cloud systems have no identity/trust relationship with any other network. This includes the iManage corporate network. Each regional network exists on its own, without a trust relationship with another region.

Patching/vulnerability scanning

Ransomware uses vulnerabilities created by poor patching and out-of-date security to find routes into a system.

- iManage Cloud is patched at least monthly, and if a vendor issues a critical patch, every attempt is made to patch on an emergency basis.
- The iManage Security Operations Center team runs scans at least once a month to actively seek out vulnerabilities.
- The iManage application security team runs internal assessments and directs external independent penetration testing.
- Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) tools are used to test changes.

Conclusion

Ransomware is a growing threat for every industry but especially for legal firms managing highly sensitive and confidential legal documents and data. They are an attractive target where the stakes are high and just the perception that a ransomware hacker could publish client information is a significant threat to a legal firm's reputation.

Law firms need to be hyper vigilant, in every aspect of their security processes, especially with training their staff. The staff will always be the weakest link in the security chain, and training them to operate safely and securely is critical but they should also be given access to highly secure applications to mitigate this risk.

The right technology with security built into its core that meets the requirements that legal professionals and law firms demand is critical. This is the iManage approach: our secure document management solution provides the safest place for lawyers to work.

To learn how your organization can protect itself against a ransomware attack, visit: https://imanage.com/solutions/law-firms/