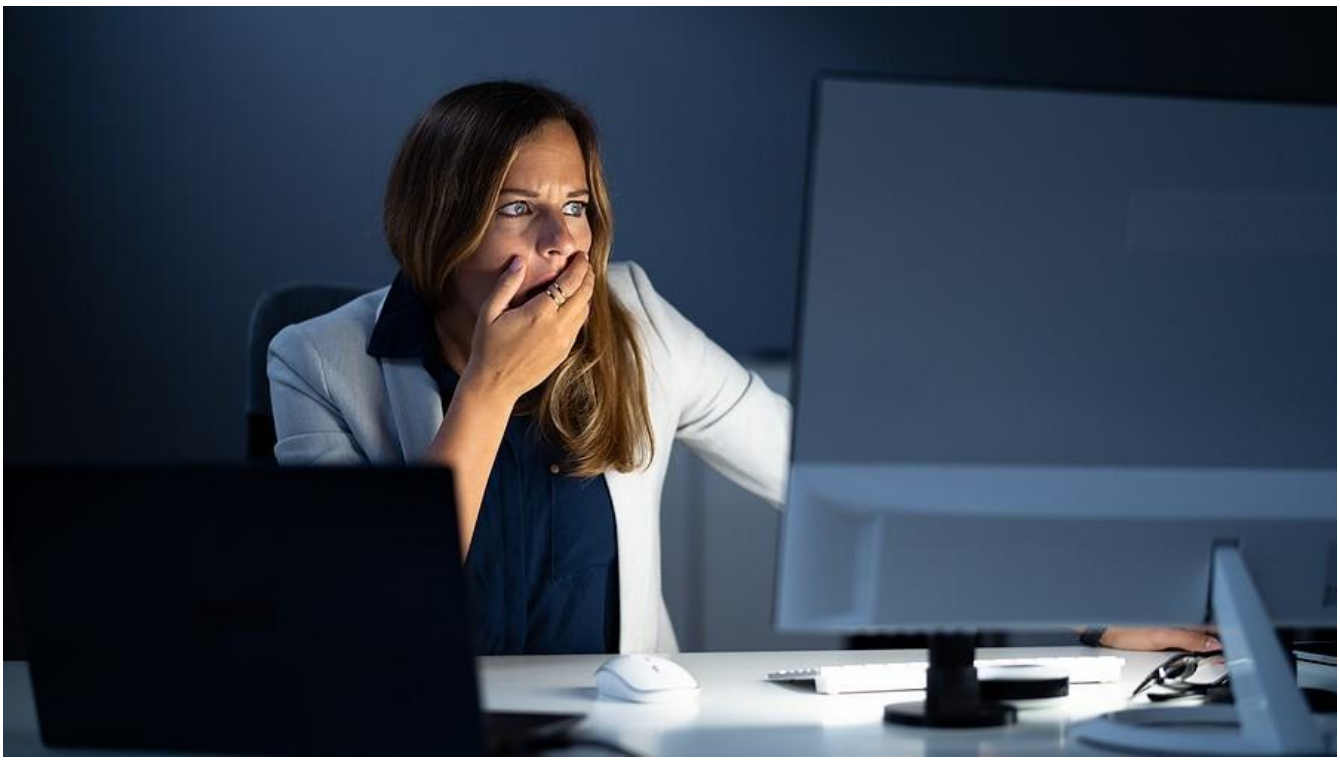
5 Steps to Prevent Cyberattacks and Safeguard Legal Client Information



Attacks like WannaCry and Petya have dominated tech news in recent years. Ransomware has become big business, with highly organized bad actors using increasingly sophisticated tactics. The risks and costs associated with ransomware have mounted higher than ever. But law firms can take simple, effective measures to prevent cyberattacks.

In the legal industry, the real costs of cyberattacks reach beyond the budget. Law firms make extremely attractive targets for hackers because they store a wealth of sensitive information. Consequently, firms have an ethical obligation to proactively address technological challenges in the context of client matters.

Catching hackers can prove nearly impossible. However, a few preventative measures will significantly reduce the threat of cyberattacks.

1. Automate Where Possible

Wherever possible, take advantage of cybersecurity automation. This includes automating mundane tasks such as patching updates. It should also include features such as file integrity monitoring and tools for threat hunting.

Hackers automate their attacks. To respond effectively, companies also need automated threat detection and response. When properly managed, cybersecurity solutions powered by AI and machine learning provide that automation, anticipating and addressing issues before they cause damage.

2. Implement Layers of Security

No single security solution will provide all the necessary protection. Implement firewalls and multi-factor authentication. Add regular data backups and ensure that end users receive targeted security training. Carefully regulate data access, particularly in a remote work environment. And be sure to implement domain name system (DNS) protection.

3. Do Not Pay the Ransom

Remember that today's hackers run a business. Victims that pay the ransom become good customers, and hackers like a good customer. That means that if you pay the ransom, your chances of getting hit a second time immediately go up.

Cyber insurance companies know this. They will suggest paying the ransom, because paying the ransom represents a relatively easy way out. But as soon as they do, you will find your policy canceled. No one else will cover you, and your firm will find itself without a safety net. Stand firm, and do not pay the ransom.

4. Apply Email Filtering and Geo Blocking

Two important preventative measures add additional security layers by stopping malware before it enters your system. Start with email filtering. With all the sophisticated technology at their fingertips,

hackers still fall back on email because it works. 94 percent of malware enters the system through email, and nearly one in three recipients open phishing messages.

Like email filtering, geo blocking stops bad actors at the door. This feature allows firms to block access from specific countries by using firewall settings or geo-based policies in Microsoft 365. For example, unless your firm serves clients in Russia, you can block inbound requests from Russian sources.

5. Conduct Regular Security Assessments

The cybersecurity environment changes almost daily. New threats emerge from the outside. Likewise, internal changes can increase risk, as well. Firms should start with an initial assessment of their technology environment and then conduct regular security assessments to identify vulnerabilities as circumstances change.

For instance, a security assessment will highlight risky password practices or identify places where unauthorized persons can gain access. To take the assessment a step further, conduct a penetration test. Pen tests involve an expert tester simulating an actual cyberattack to identify weaknesses.

eMazzanti Uniquely Positioned to Help Prevent Cyberattacks

The legal IT experts at eMazzanti bring a powerful skill set to the table for their clients. With deep experience in cybersecurity best practices, we have secured thousands of businesses and legal firms.

Schedule an initial risk assessment and then work with our consultants to customize a cybersecurity solution tailored to your environment. Our eCare Secure Route delivers the automation you need, with comprehensive threat detection, predictive intelligence, and proven reliability.