# PROTECT YOUR LEGAL DATA FROM CYBER ATTACKS

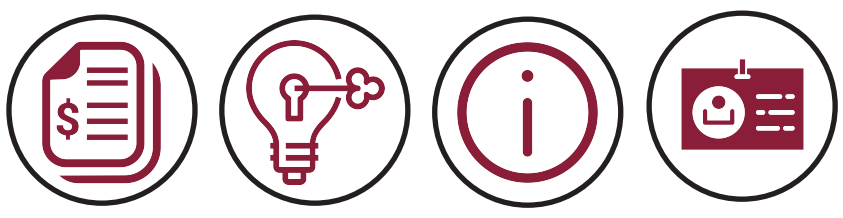
*Cyber attacks can occur anytime. In a recent study by LogicForce, over 50% of 200 law firms do not have a cyber attack response plan and 66% reported cyber infringement.*

## UNDERSTAND SECURITY STANDARDS

Threats affecting law firms include:

- Email phishing attacks
- Impersonation of executives
- Potential data loss
- Extortion via ransomware

The ISO 27000 protects:



*Financial Information* | *Intellectual Property* | *Third Party Information* | *Employee Details*

## TAKE USER TRAINING

*Train your team by using online resources.*

Everyday:

- 156 million phishing emails sent globally
- 16 million make it through spam filters
- 8 million emails are opened
- 80 thousand people fall victim to a phishing scam

## DEVELOP POLICY & PROCEDURES

*Establish proper use of a firm's technology resources.*

The ABA offers models for:

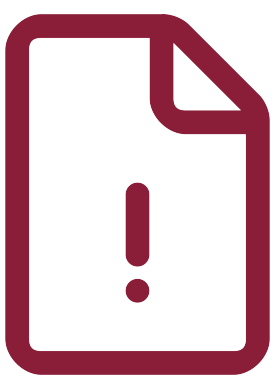
- Social media policies
- Document retention policies
- Disaster recovery plans
- Incident response plans
- Mobile security policies

## ENSURE BUSINESS CONTINUITY

*You can lose your files in event of a disaster.*

Disaster recovery programs include the following to prepare for unseen problems:

- Governance
- Testing mechanisms
- System documentations

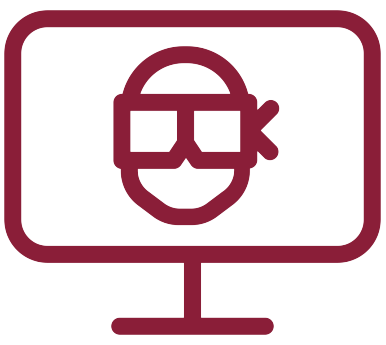


## REVIEW INTERNAL SECURITY

*Hackers can steal confidential information.*

Combat cyber attacks by adding:

- Endpoint security agents
- Firewalls
- Internal intrusion detection sensors.

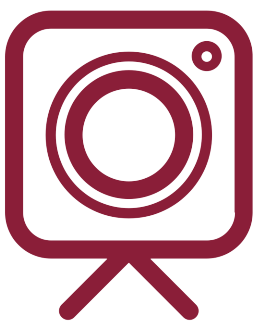


## ADDRESS PHYSICAL SECURITY

*Protect your clients and your practice by taking physical security measures.*

Below lists important physical security measures:

- Keycard access
- Security cameras
- Visitor IDs



*Attorneys are responsible for keeping data safe. With the help of technology, cyber attacks can be prevented as can data loss.*