Protect your firm and clients: Top 10 cybersecurity steps for law firms



Candor. Insight. Results.

Protect your firm today from tomorrow's breach

Law firms historically are entrusted with highly confidential data, which makes them prime targets for today's cyber criminals. Protect your firm—and your clients' information—from cyber threats with these cybersecurity steps and avoid compromising sensitive information and damaging your reputation.

Logging and monitoring

Basic protection:

Select your top four to seven security events to log and then set up alerts when the events are triggered

Advanced protection:

Implement a security event monitoring system/service

Basic protection:

Purchase quality cyber liability insurance

Advanced protection:

Create an incident response plan, including a multidisciplinary response team and then test against the plan for weaknesses

Disaster recovery

Basic protection:

Replicate critical systems and data to off-site data center

Advanced protection: Virtualize server and network infrastructure

Audits/assessments Basic protection:

Get an independent thirdparty to evaluate your cybersecurity practices

Advanced protection:

Develop an annual audit/assessment plan, including quarterly vulnerability scanning

Networks

access

Basic protection:

Use firewalls with restrictive settings to protect critical systems

Advanced protection: Restrict wireless network

Mobile devices

Basic protection:

Require passcodes and encryption on all devices

Advanced protection: Set up remote wiping capabilities on all devices

Incident response

Top 10 **Cybersecurity Steps**



User access

Basic protection:

Be authoritarian with

adding, modifying, and

removing all user access

Advanced protection:

Implement two-factor

authentication for all

users

Training

Basic protection:

Frequently communicate cyber threats and proper practices to users

Advanced protection:

Test user compliance using simulated threats and reward users who act responsibly

Vendor management

Basic protection:

Require vendors to annually certify their cybersecurity practices

Advanced protection:

Develop a robust vendor management process including cybersecurity service level agreements and audits

Encryption

Basic protection: Encrypt all laptops and

desktops

Advanced protection: Encrypt databases with critical and regulated data

Baker Tilly's cybersecurity and professional services industry teams can help you assess your current cyber-risk profile on the roadmap or tailor a customized plan unique to your law firm environment. We can give you the tools to protect your law firm today from tomorrow's cybersecurity breach.

Visit **bakertilly.com** to learn more.

An independent member of Baker Tilly International