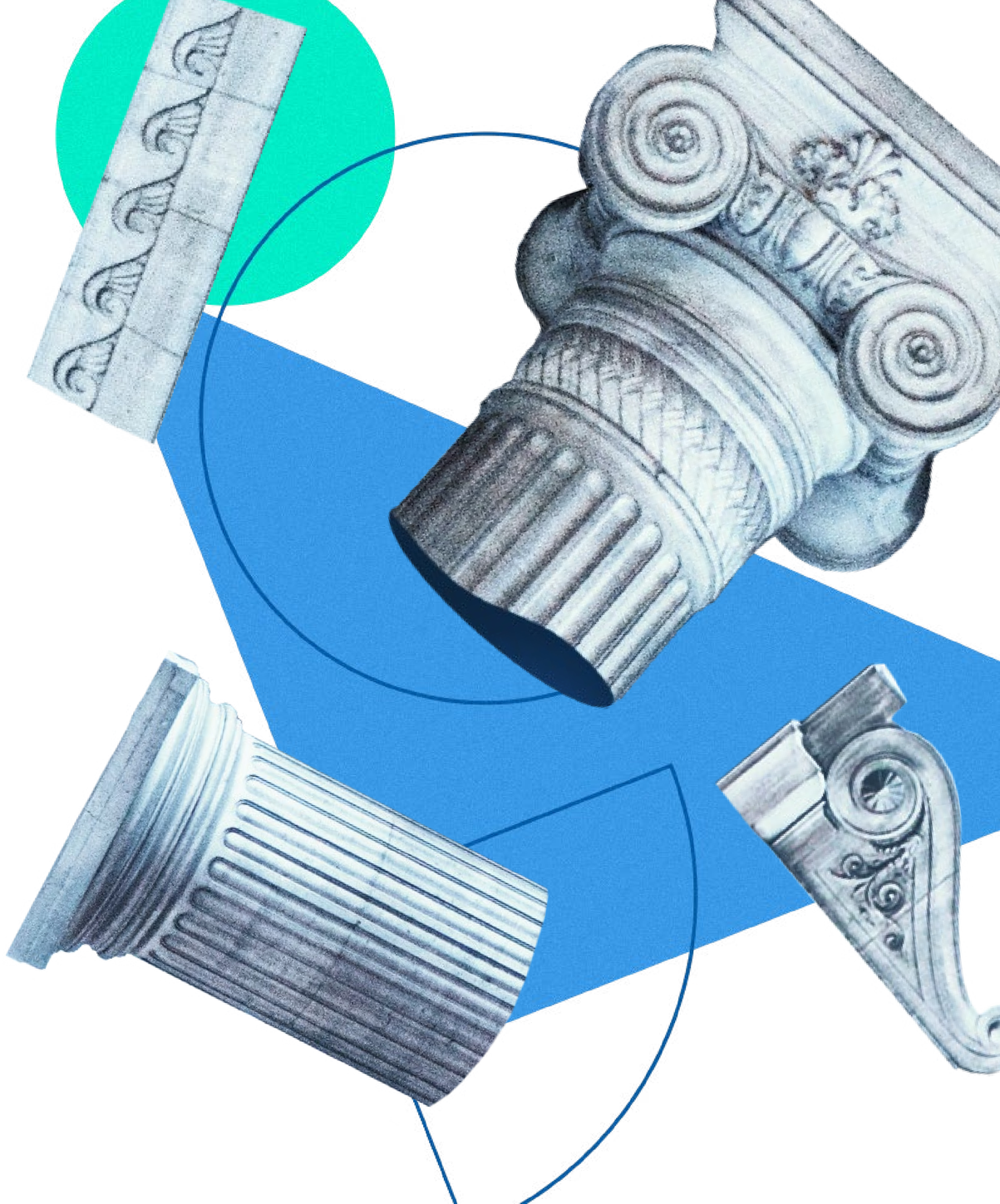
FIELD EFFECT™

Law Firm Cyber Security: 10 Mistakes to Avoid



2020 was a cyber security wake-up call for law firms. In the US, nearly one-third[1] of attorneys experienced a security breach. In the UK, 75%[2] of attorneys reported they'd been targeted by cyber criminals.

Discover ten critical cyber security mistakes law firms should avoid — plus steps you can take to build a better defence.

01

Thinking your firm is too small to be a cyber crime target.

Every law firm is a potential target for cyber crime — regardless of size. In fact, small and mid-size firms are even more vulnerable, with 58% experiencing a ransomware incident in 2021 alone.[3] Smaller firms may lack the cyber security resources to keep their confidential data and intellectual property secure, which makes them a prime target for attack.

02

Relying too much on traditional security.

Your cyber security measures must protect work, no matter where it takes place. Traditional security tools, like firewalls and antivirus software, won't provide the strong protection or scalability you need for modern workforces. Look for complete, advanced security solutions that can identify threats early across your entire IT infrastructure — including your network, endpoints, cloud services, and remote workers — and provide the capabilities to respond quickly and effectively.

03

Not adopting a zero-trust security model.

Firms that still use an open security model, where all users on a network have equal access to confidential information, are increasing their risk of a cyber attack. The zero-trust model means that access to information is kept on a need-to-know basis. All users must be authenticated and authorized to login to portals and applications or to view, manage, and edit data.[4]

04

Not enabling multi-factor authentication.

Enabling multi-factor authentication adds another layer of defence to password protection,[5] requiring a second (and even third) step to verify the user's identity. This could be a one-time code via an app (such as Google Authenticator or Microsoft Authenticator), SMS message, or even a biometric token like a fingerprint. When used as part of a complete approach to cyber security, MFA can prevent up to 99.9% of all automated cyber attacks and 75% of targeted attacks.[6]

05

Lacking visibility across your IT infrastructure.

Without insight into your threats and an effective way to respond, your firm may be at risk of an attack that could significantly impact all you've worked hard to establish. Building visibility across your IT infrastructure requires tools that allow you to monitor and detect suspicious or abnormal activity early. In turn, this complete view lets you stay ahead of cyber risks, identifying and closing gaps before an attacker can exploit them.

06

Not applying software patches and updates fast enough (or at all).

Patching and updating software as soon as possible mitigates cyber security vulnerabilities and ensures your systems are safe. Every minute systems are left unpatched is another your firm is at risk. Develop a policy and plan for managing updates quickly as possible.

07

Overlooking third-party vendors and their cyber security risks.

Your network of vendors — including cloud service providers such as DropBox, DocuSign, and Clio — represents another potential security risk. If their security defence is lacking, it could give cyber criminals another access point for attacking your firm. Take the time to assess any prospective vendor's security posture before working with them.

08

Having no incident response plan.

Is your firm ready to respond to a cyber security incident? Planning and rehearsing incident response is vital for mitigating an attack's impact while ensuring business continuity. Take the time to define remediation steps, resources needed, and the processes your team will follow to respond quickly and effectively.

09

Providing cyber security training for only a select few.

From the managing partners to the front desk receptionist, everyone at a law firm needs to have a solid understanding of cyber security basics. Unfortunately, cyber training often gets relegated to the IT department. Make sure everyone knows how to spot a phishing email, what to do if they clicked a malicious link, and how to securely send files.

10

Tackling cyber security alone.

Cyber security can be costly, time-consuming, and complex, especially if firms try to do it all in-house without the necessary expertise.[7] The good news is you don't have to do it alone. Look for a cyber security expert that can provide a complete approach with the tools and support to keep your firm secure.

Were these tips helpful?

Share it with partners or colleagues who may want to learn more about improving security for their law firm. If you have any questions about steps your practice can take to defend against cyber threats, our experts are here to help.

Sources

1 https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/
2 https://www.sra.org.uk/sra/how-we-work/reports/cyber-security/
3 https://blog.capterra.com/law-firm-ransomware/#methodology
4 https://securityboulevard.com/2020/07/zero-trust-security-model-what-you-need-to-know/
5 https://www.akingump.com/a/web/51258/RPRT-RM10.16-5-Cybersecurity.pdf
6 https://cybertechaccord.org/multi-factor-authentication-mfa-a-foundational-cyber-defense-for-organizations/
7 https://fieldeffect.com/blog/law-firms-major-targets-for-hackers/

fieldeffect.com
hello@fieldeffect.com

Canada and the US
+1 (800) 299-8986

United Kingdom
+44 (0) 800 086 9176

Australia
+61 1800 431418

FIELD EFFECT