Why IT Must Take Control Over User Risk

Takeaway from the ILTA/Conversant Group Cybersecurity Survey of Law Firms

In today's law firms, most IT professionals view user behavior and lack of training to prevent these behaviors as the top risk to security (according to our recent International Legal Technology Association/Conversant Group study). Indeed, user behavior/training arose as a greater concern than ransomware or any threat actor tactic that would exploit these key drivers of organizational productivity.

However, there is one unassailable truth: users are human, and they will *always* be fallible no matter how much training you throw at them. Thus, blaming them or exercising an extreme focus on securing their behaviors will not lead to defensive actions that secure the organization. In cybersecurity, simple solutions rarely solve holistic problems. Firm IT, with support from leadership, must take a stronger stance to defending systems—assuming users will make mistakes—while also training these users to reduce risk on multiple fronts.

So, What Defensive Actions Can Firms Take?

Our data sheds more insight here as well. Users only present risk when they click the wrong link, open the wrong attachment, access the wrong website, or conduct other risky behaviors. Firms can dramatically reduce these risks by using controls that eliminate these options from users entirely. Many of today's firms expect users not to engage in risky behaviors but still enable those behaviors. This would be like an airport TSA checkpoint listing forbidden, hazardous materials, but failing to scan for them, putting the onus of security on the traveler.

From our survey data:

- 90% do not block or restrict external file hosting sites.
- 72% do not automatically enforce encryption of email through content examination.
- 43% do not enforce encryption of removable media.
- 79% require fewer than 16-character passwords.
- 20% do not have deep packet inspection configured on their firewall.
- 38% do not block malicious sites at the firewall.
- 33% have not enabled anti-spoofing/impersonation protection in the spam filter.
- 24% do not run AV scans on inbound email.
- 80% do not provide a password vault to users.
- 20% have no form of MFA on user accounts.

Simply put, threat actors exploit users because organizational controls allow them to.

Stop Allowing, Start Blocking by Default

The recommended remedy is to stop allowing and start blocking. Otherwise, firms are making security optional, at the whim of human foibles with potentially disastrous consequences.

Firms should move toward a policy of Zero Trust: trust no one and nothing by default. As examples, choose one IT-vetted password vault and block all others; choose one browser and block all others; choose one file sharing platform, and by default, block all others (and so on). All necessary exceptions should be tracked on a Risk Register. Once a threat actor takes control of a user's endpoint, the user endpoint and threat actor become synonymous in how freely they can move throughout and access your systems. Systems are simply not designed to detect and block a threat actor accessing systems from an approved device and user account: systems are open by default. Thus, the tools a firm might purchase for remote control, like Screen Connect, SolarWinds, Manage Engine, Bomgar, etc., can also be used by a threat actor for the same. Risks must be managed from this paradigm: if a user or IT admin can do it, assume that a threat actor can as well.

It's Time for IT to Take Control—Led from the Top Down

We recognize these controls require an investment and that leadership is often resistant to sweeping changes; similarly, IT teams must bear the burden of convincing these leaders that the costs and user inconveniences are needed to secure their firms against user risk. But in 2022, over 100 law firms reported sensitive data breaches to state authorities (according to a report by Law360), up 14% over 2021 and 117% from 2020. The data lost can be material to corporate business and sensitive to clients' personal and financial wellbeing. The incidents themselves can cause significant financial losses, and even business insolvency. To complicate issues for law firms, releasing client confidential information is a violation of the ethical standards to which lawyers have agreed and can result in malpractice and class action lawsuits. In January and February of this year alone, malware groups began specifically targeting law firm employees, attacking some firms with targeted threat campaigns, according to eSentire. Organizing firm defenses against these threats rather than around user convenience is an essential step to mitigating this considerable area of vulnerability. Users must be educated on why these controls are necessary, shifting the paradigm of the law firm security approach away from users and toward stronger controls. We are not arguing that systems should not be usable; however, we are arguing that users must grow accustomed to many behaviors being blocked by default and following an exception process when a specific action is required for business.

So, Are Users Really the Problem? Can Firms "Secure the User" to Prevent a Breach?

Emphatically, no. The core issue is that systems are open by default, and this configuration must change. Additionally, many law firms have not invested in adequate security operation center services and lateral movement/backup defenses to prevent a non-recoverable mass destruction event. But they should consider them for a more comprehensive security program.

About the Conversant Group/International Legal Technology Association (ILTA) Cybersecurity Survey and Report

In 2022, Conversant Group and ILTA collaborated to conduct the first-ever cybersecurity-focused benchmarking survey for the legal industry. The survey was targeted specifically at understanding cybersecurity controls, tools, practices, and assumptions in law firms. The results were presented in the report, "Security at Issue: State of Cybersecurity in Law Firms," available for download now. This snapshot presents one key takeaway from the report.