Shadow IT: A Serious Threat to Law Firms

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

What is Shadow IT?

The first problem with cautioning lawyers about the dangers of shadow IT is that most of them have no earthly idea what it is. So let's start there.

Gartner has defined Shadow IT as meaning IT devices, software, and services (including cloud services) outside the ownership or control of the IT department of a business.

Once lawyers understand the definition, they generally say that everything is within the control of their IT department. Most of the time, that answer would be wrong, though many don't know it.

Just the Facts Please

Studies by Gartner have revealed that Shadow IT constitutes an amazing 30-40% of IT spending in big enterprises. Advisory firm CEB estimates that the right percentage is 40%. Everest Group research states that it makes up 50% or more of the spending. No need to split hairs – all three numbers are big.

Small law firms are not immune to this trend. How many law firm services are in the cloud, especially today? And are they all under the control and direction of the IT department? The likely answer is no.

Are They All Renegades?

Absolutely not. In fact, Shadow IT is sometimes implicitly permitted or even encouraged. Many would argue that Shadow IT makes businesses more competitive and allows for enhanced collaboration and innovation. In their view, users discover applications or services that allow them to do their jobs better or more easily, and IT can subsequently go in and secure the applications or services. In our experience, this is not a useful way to approach risky behavior by employees, the consequences of which can be dire.

Why do employees "go off the reservation?" Sometimes, the IT department moves slower than the average tortoise or routinely raises objections to what employees want to do. Undeterred, employees make an end-run around the rules – it is generally simple for those who have access to data to put it where they want and use it as they wish using tools or services that may not be authorized.

IT departments are often burdened by having a limited number of employees and constant demand for providing services. Sometimes, those who are outside of the IT department are pretty sharp technologically – and running Shadow IT operations doesn't intimidate them.

Cloud services and other vendors make it darn easy to implement new solutions. Just think about artificial intelligence – once it was complicated to implement, now it is so easy that solo/small practitioners do it all the time.

Can't You Control Shadow IT by Policies or Technology?

Absolutely not. Ignoring policies is routine in most places. Employees know what they want to do and policies frequently do not deter them. Often, they think the evasion of the policy is good for the law firm, that it allows for better solutions.

A good example is Dropbox, where we see many e-discovery productions made, usually without encrypting the data first before sharing it via Dropbox. There may be a policy against using Dropbox without encrypting sensitive data first, but many lawyers will ignore that policy. Using technology to block access to Dropbox is possible but very unpopular with lawyers, who do indeed have many uses for it that do not involve sensitive data. The consequence is that blocking is discarded as a solution, with IT relying on the policy instead. And we've seen how well that goes.

This puts the IT department in a difficult position. They mandate "don't do this," someone does do it – and there is no apparent harm. We say "apparent harm" because often the Shadow IT solutions are riskier. They are not vetted by the IT department which is responsible for ensuring the law firm's security and compliance with any number of laws and regulations. Is it a conundrum? Absolutely. IT often attempts to block certain applications, but the ability of employees to find a way around the blocking is uncanny. Shucks, if Dropbox is blocked, not a problem. Google Drive, OneDrive, or any other cloud storage will work just fine.

A New Enemy in Town: Shadow Policies

Security experts have worried about Shadow IT for a long time, but now they must add shadow policies to the mix. The larger the law firm, the more prevalent shadow policies are. They are rogue policies written by a particular group or department that are never reviewed, approved, and made part of the law firm's policies.

And yet, they expose the law firm to legal liability by setting their own duty of care to employees. If something goes south and rogue policies are discovered, the doors of legal liability may be thrown open. Many shadow policies are written by people who are not experts at writing policies – without review, they often bear little relation to the law firm's official policies – and yet an entire department may abide by them.

Shadow policies were spurred by the pandemic, with collaboration between distinct groups becoming more intense. Perhaps it was natural that they sought to write their own policies.

As crazy as it sounds, there needs to be a policy on writing policies. Why? Because it establishes the framework of policy management, sets forth how policies should be written and approved, etc.

All policies should be in one place where all employees know they can find them. Train employees: If they discover a shadow policy that is not in the centralized policy list, they need to report that policy.

Battening Down the Hatches

In a June 2021 study by security company Hysolate, the authors stressed what seems inevitable from the data cited above. Employees need both more freedoms – and more restrictions. Moreover, almost all of those surveyed by Hysolate reported that their 2021 budgets included addressing remote IT challenges, including Shadow IT.

One statistic caught our attention. Only 7% of users do not complain about security restrictions, but the remaining 93% look for ways to bypass them. With that mentality, we can certainly understand how hard it is to contain Shadow IT.

The goal is to batten down the hatches while allowing increased employee IT freedom. 87% of respondents want to increase employee IT freedoms while 79% want to increase employee IT restrictions. IT respondents want to afford employees more freedom (the major freedoms being to browse the internet freely, installing 3rd party apps and plugins, printing at home, and performing personal activities on work devices), but to do them securely. And therein lies the heart of the problem. Can law firms give employees more IT freedom securely? Can they really batten down the hatches?

The upside, according to the survey, is that most people believe that enhanced IT freedoms will increase employee productivity, make IT policies more palatable and reduce employee frustration.

The authors question whether the price tag of IT freedom is an increased danger to the law firm's confidential data, but then we admittedly look at everything from a security vantage point. We shudder at the installation of unapproved apps and using endpoints for personal activities. The counterargument is that it may be possible to use endpoint privilege management, application isolation, and browser isolation to secure IT operations by employees.

Final Words

As last year's Hysolate 2020 report noted in *The CISO's Dilemma,* IT and security leaders then viewed worker productivity and enterprise security as mutually exclusive objectives. The pandemic appears to have changed that view. At this point, there is a strong push to use isolation and privilege management technologies to afford security AND IT freedom.

In conclusion, we may start to see Shadow IT come out of the shadows in law firms with the blessing of IT. Everyone is looking for solutions to the risks presented by Shadow IT – it remains to be seen if they can successfully utilize technology and processes that afford secure employee IT freedom. And to add another thought to the mix, perhaps law firms should be investigating Zero Trust Network Access (ZTNA) instead of battling Shadow IT.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* snelson@senseient.com

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker, and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity, and digital forensics services from their Fairfax, Virginia firm.* jsimek@senseient.com.

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker, and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* mmaschke@senseient.com.