Bad News About Lawyers' Income – and Their Feckless Cybersecurity

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

Straight From the Headlines

Most of our IT, cybersecurity and forensics clients are law firms, so we were struck by new data we received that will likely interest (and depress) all lawyers.

As Reuters reported, it turns out that lawyers make less money today than they did in 2001 when inflation is accounted for.

So . . . the median annual income of U.S. lawyers dropped almost 2% from $129,389 in 2001 to $126,930 in 2020. That data comes from a paper which will be published in an upcoming edition of *The Journal of Economics and Finance*.

The rest of U.S. workers, again accounting for inflation, increased their purchasing power by almost 4% during the same time period.

The study relies on national lawyer earnings data from the U.S. Bureau of Labor Statistics. No surprise here, but solo practitioners and those lawyers in government and non-profit settings make significantly less than lawyers at large firms.

Across all sectors, the data indicates that lawyers' median real income peaked at $134,005 in 2010 and has gradually declined since then.

More Gloom in Your Future?

For many lawyers and law firms, the probable answer is yes.

The study concluded that there are too many lawyers – and they are facing a declining demand for legal services.

The data shows that legal services made up 0.58% of U.S. gross domestic product in 2001 and reduced to 0.28% in 2019. Sadly for lawyers, Americans are spending proportionally less on legal services now than they were two decades ago.

Why? There are many reasons. Many legal tasks are automated, you can buy inexpensive forms online, there are more paralegals and fewer lawsuits in some areas – litigation is expensive, as we all know. The number of lawsuits filed in federal courts has declined on both per capita and per lawyer bases since 2001.

And yet, lawyer ranks keep growing. The number of lawyers per every 1,000 workers in the U.S. went from 4.15 in 2001 to 4.4 in 2019. Which means more lawyers are fighting for a slice of an increasingly smaller pie.

At the top of the heap, the AmLaw 100 are doing just fine, reaping ever-growing profits from the cream of the corporate crop. In other words, the gap between the "top dogs" and everyone else is widening.

And to Cheer You Up (Not), Here's How Lawyers are Paying for Their Shoddy Security

Just when we thought ransomware might settle down a bit, we continue to see successful ransomware attacks in all sectors. Let us try to lend a helping hand. Microsoft has released its second edition of Cyber Signals, highlighting security trends and insights gathered from Microsoft's 43 trillion security signals and 8,500 security experts.

Microsoft analyzed anonymized data of real threat activity - it found that over 80% of ransomware attacks can be traced to common configuration errors in software and devices.

What are law firms (and everyone else) doing wrong?

They leave applications in their default state, allowing user-wide access across the network They use security tools which are untested or misconfigured. They have cloud applications set up in a way that permits attackers to gain access to their networks. Also, they do not apply Microsoft's attack surface reduction rules, which allows attackers to run malicious code using macros and scripts.

The misconfigurations cited above are precisely what ransomware attackers are looking for. Do not leave those doors open, especially now that ransomware attacks frequently involve double extortion – seeking monies for a decryption key as well as stealing data which they threaten to release unless a second ransom is paid. And even if you pay, the data may still be released. Happens all the time. What's your recourse then? You have none.

The Rise and Wrath of RaaS

Microsoft warns of the growth of the ransomware-as-a-service (RaaS) ecosystem, which permits attackers who do not have a lot of expertise to create and develop their own ransomware to conduct ransomware attacks.

RaaS kits are child's play to find on underground forums and they now include customer support, providing criminals with all the assistance they need to get started. Some of these ransomware kits are sold via a subscription model, while others are affiliate models, where the sellers get a piece of the action from each ransom payment.

As Microsoft accurately notes, "ransomware is an avoidable disaster. Reliance on security weaknesses by attackers means that investments in cyber hygiene go a long way."

Recommendations From Microsoft You Should Heed

So, what should you being doing? Microsoft recommends closing security blind spots by ensuring that cybersecurity tools and procedures are configured correctly in a way that protects your systems. You must also disable macros and other scripts that cyber criminals often exploit to execute malicious code. In an attempt to protect users from themselves, Microsoft now blocks macros in Office apps by default.

Of course, everyone should be using multi-factor authentication (MFA), everywhere it is available. We are regularly astonished by the pushback of lawyers who simply don't want to be troubled by having a second factor. Trust us, it becomes second nature to you to use MFA and some methods of using multi-factor authentication are quite simple. Just remember how darn effective it is at preventing mischief in your network! Your cyber insurance carrier may even require MFA, again trying to protect you from yourself.

Think about how easy it is for cybercriminals to use stolen IDs and passwords to move around the network in their nefarious schemes, particularly ransomware attacks. The use of MFA stops nearly all of those attacks.

And let us not forget what makes us tear our hair out, finding law firms that are not applying security patches and updates quickly upon their release. It is only hours (or minutes) after a vulnerability becomes public that the cybercriminals seek to exploit it. Do not aid and abet them by dragging your feet when it comes to patches and updates! That way lies disaster . . .

***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 (CISSP), Certified Ethical Hacker (CEH) 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.*