What Insurers Want to See: Practical Steps to Reduce Your Cyber Insurance Costs

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

Cyber insurance used to feel like a checkbox. Get a policy, file it away, and hope you never need it. That era is over.

Premiums have risen, underwriting has become stricter, and carriers are asking for much more detailed information about how companies operate. Insurers are no longer just setting policy prices; they are assessing risk in real time, and companies that can't demonstrate strong security controls are paying the price.

The good news is that cyber insurance pricing isn't random. Companies that take specific, measurable actions to cut risk can often lower premiums and get better coverage terms at the same time. The key is understanding what insurers truly want.

Insurers are Pricing Behavior and Not Just Technology

Insurers are focusing less on what tools you claim to have and more on how your firm behaves.

For example, multi-factor authentication is no longer just a nice feature; it is now often a basic requirement. Companies that do not implement it for email, remote access, and administrative accounts are considered high risk.

The same applies to password management. Weak or reused passwords remain one of the easiest ways for attackers to gain access, and insurers expect companies to enforce stronger credential practices, such as using password managers and similar safeguards.

These are not advanced cybersecurity measures; they are foundational.

Your Employees Are Still the Biggest Risk

It’s important to reinforce something that most firms already know but still underestimate - human error drives most incidents.

Training employees to recognize phishing emails, suspicious links, and social engineering attempts is one of the most effective ways to reduce both the risk of breaches and insurance costs. From an insurer’s perspective, a company that conducts regular security awareness training and phishing simulations is substantially safer than one that relies only on technology. This difference influences underwriting decisions. For law firms, this is especially crucial, as attorneys and staff handle sensitive client communications daily, making them prime targets for well-crafted phishing attacks.

Maintenance Matters More Than New Tools

Another consistent theme is that basic system maintenance directly impacts premiums.

Keeping software up to date, applying security patches, and maintaining current systems are among the simplest ways to reduce exposure. However, these practices are often overlooked. Insurers know that many successful attacks target known vulnerabilities that were never patched. Companies that can show consistent updates and maintenance procedures have a lower risk profile.

This is not about buying more technology. It is about properly managing what you already have.

Security Controls Are Now Tied to Coverage

One of the more important shifts in the market is that insurers are no longer offering broad coverage without conditions.

They are asking detailed questions about cybersecurity controls during the application process. Sometimes, they carry out vulnerability scans or require specific safeguards before issuing or renewing a policy. This means that gaps in your security program are no longer just internal concerns; they directly influence whether you can get coverage and at what cost.

For law firms, this creates a new dynamic. Cybersecurity is no longer just about preventing incidents; it's about preserving insurability.

Incident Response Planning Is No Longer Optional

Another area insurers increasingly evaluate is incident response preparedness.

Having a documented and tested incident response plan indicates that a firm can effectively contain and manage an event. This reduces potential losses, which in turn lowers the risk from the insurer's perspective.

Firms that cannot demonstrate a clear response process may still qualify for coverage, but often at higher premiums or with more restrictive terms. Essentially, this involves knowing who to contact, how to isolate affected systems, and how to communicate both internally and externally when an incident occurs.

The Bottom Line

Cyber insurance is no longer a passive purchase. It is an active reflection of your firm's security posture.

Firms that invest in foundational controls such as multi-factor authentication, employee training, system maintenance, and incident response planning are not only more secure but also more insurable, often at a lower cost.

Those firms which don't' make these investments will continue to face higher premiums, fewer coverage options, and greater scrutiny from carriers. For law firms, if you want to pay less for cyber insurance, you need to appear to be a lower-risk client. And that starts with doing the basics well.

Michael C. Maschke *is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.*

Sharon D. Nelson *is the co-founder of and consultant to 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 the co-founder of and consultant to Sensei Enterprises, Inc. He holds multiple technical certifications and is a nationally known digital forensics expert. He is a co-author of 18 books published by the American Bar Association. jsimek@senseient.com.*