Breckenridge®
an accretive company

Problem solvers found here

CYBER HAS GONE LOCO!

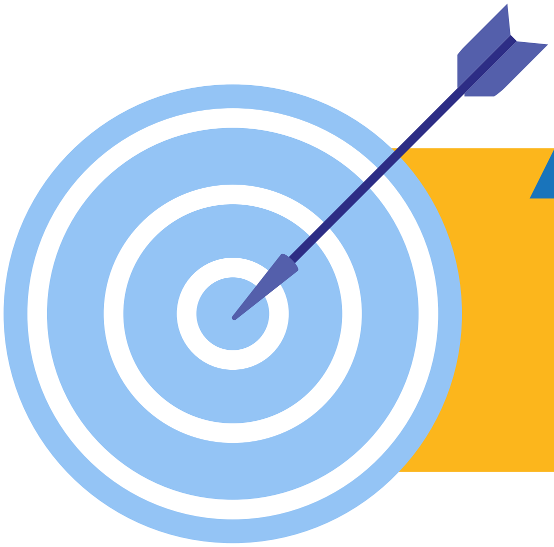
In this current ultra-hardening cyber market, which also affects the Technology E&O market, it is extremely important to talk with your insureds about their security controls and risk management for their cyber exposures well in advance of the renewal of their coverage. Many carriers are re-assessing their entire books of cyber, changing terms, decreasing coverage, and increasing rates.

Conditional Renewals and Non-Renewals are commonplace

Some of our carriers have sent conditional renewal or non-renewal notices on their entire cyber book to allow them the ability to re-underwrite each risk. Keep in mind, this is a courtesy in the case of E&S carriers who, in most states, do not need to give any notification to non-renew an account. Capacity (limits available) is shrinking, underwriting guidelines are severely tightening and rates are increasing. To avoid any problems, we also recommend that renewal submissions are submitted at least 30 days prior to renewal, and if possible, 60 days prior. This will allow time to remarket and/or obtain XS should this be needed.

Excess Cyber Often Required

Even with limits as low as $5MM, it is often necessary to layer coverage. Many carriers are cutting back to a max of $2MM-3MM per insured in the first $10MM – which carriers still consider the "burn layers" given recent claims activities. (Burn layers = limits that are more highly exposed for a claim.)



We still have solutions

We have a multitude of cyber and tech carriers and will thoroughly shop your renewal as warranted to get the best possible terms for you. We have nearly 40 markets when you consider several Lloyds syndicates. We are well versed in finding and coordinating limits to help respond to your insured's cyber needs.

Preparing your risk to be a "best in class" cyber insured

If you can present your potential risk/insured to be a best-in-class risk, the renewal (or new business marketing) for their cyber coverage will go much smoother. Putting yourself out there as a risk manager is nothing new for agents; putting yourself out there as a cyber risk manager will give you an advantage.

Some of the security controls and cyber risk management that most (if not all) carriers are requiring to renew/write coverage are on the next page. The larger the size of a risk/insured or the higher exposure the risk/class of business is, the stricter the carriers will be about these controls.

If you have any questions about your specific risk/renewal, please let us know.

Security Controls Carriers May Require for Coverage

- Multi-Factor Authentication (MFA) – this will be required not just on email or remote access, but an additional layer for accounts with administrator privileges and should include MFA for all systems.
- Email Filtering:
  - Tagging of external emails
  - Multi-layer email filtering
  - Screening of emails for malicious attachments
  - Sender Policy Framework (SPF)
  - Domain Keys Identified Mail (DKIM)
  - Domain Based message Authentication, Reporting and Conformance (DMARC)
- Updates/patches to fix vulnerabilities such as Log4J, Solar Winds, etc.
- Regular updates of MS/Operating System patches and updates
- Use of Remote Desktop Protocol (RDP) when remote access is allowed
- Data Encryption
- Use of Next Generation Antivirus (NGAV)
- Use of Endpoint Detection and Response (EDR)
- Use of Privileged Account Management Software (PAM) -i.e. CyberArk, BeyondTrust, etc
- Active monitoring of admin accounts for unusual patterns
- Hardened baseline configuration across servers, laptops, and managed mobile devices
- Use of a Protective DNS Services (PDNS) – eg Zscaler, Quad 9, etc. to block access to known malicious websites
- Endpoint application isolation and containment technology for all endpoints
- Security Information and Event Management System (SIEM)
- Utilization of a Security Operations Center (SOC) that is managed 24/7 (outsourced or inhouse)
- Use of a Vulnerability Management Tool
- Regular backups that are encrypted and stored off site/off network
- Securing/Closing of any open ports

Is this list all encompassing?

No – absolutely not. These items are ever evolving and more could be asked of your insureds as technology advances. The hackers are always evolving, and security measures need to keep up with this evolution.

When should I have these conversations?

As you can see, this is quite extensive and overwhelming – it will be nearly impossible to implement in less than 30 days. Starting the risk management conversation early with your insured allows them to be prepared for the renewal. In most cases, carriers are not willing to extend or bind “subject to” these items being done.   Our recommendation is that these conversations be started at a minimum 90-days prior to renewal and as soon as 180 days (six months) prior to renewal to allow time to implement any security controls not in place.

Questions? Need more resources?

We are always available for questions about your insureds’ upcoming renewals. Please feel free to use this paper as a guide to have discussions with your insureds. We have also set up a cyber risk management page on our website here. This page includes resources, links to webinars and a link to our comparative cyber rater, where you can quickly get indications for cyber from up to 10 carriers.

Call us. Email us. Reach out today.
We can get you through this bubble burst, if you take the first step.

Victoria Dearing
MBA, AAI, CPCU, RPLU, ARM-P
SVP Professional Liability and Risk Management
469.320.4033
vdearing@breckis.com