SUN DOG

CYBER INSURANCE IS A BREEZE WITH A STRATEGIC IT PARTNER

A QUICK REFERENCE GUIDE

Cyber risk is constantly evolving, making it difficult for insurers to develop consistent risk profiles. Using our experience helping customers in diverse industries with unique insurers, we’ve identified common themes and frequently asked questions. **Use this document to help proceed with confidence as you apply or renew your cyber insurance policy!**

While every insurer is different, the security systems and practices underwriters look for when evaluating risk and pricing out policies remain fairly constant.

TOP SECURITY CONTROLS FOR CYBER INSURANCE:

PRIVILEGED ACCESS MANAGEMENT (PAM)

Solutions to control, secure and audit access to privileged accounts (root, superuser, etc.) used by system administrators and other privileged users. Privileged accounts are typically used for a limited and defined time (i.e., just-in-time) and by approval or workflow.

MULTI-FACTOR AUTHENTICATION (MFA)

Solutions to positively confirm the identity of remote workers, as well as privileged users like system administrators and third-party IT management vendors. MFA has emerged as a fundamental requirement.

DATA BACKUP AND RECOVERY BEST PRACTICES

To ensure businesses can quickly restore operations in the wake of a cyber-attack or disaster.

DON'T KNOW? DON'T GUESS!

By nature, there are going to be some technical questions on your insurance application. If you don’t know how to answer a question, just ask us! We’re happy to clarify.

IT IS OKAY TO SAY NO.

There will be sections that your company will likely answer ‘no’ to. Focus on the baseline requirements and work towards the best-in-class recommendations that fit your needs.

DON'T PROCRASTINATE

Keeping in mind the sheer complexity of some of these requirements, it is crucial to start your application sooner than later so if you’re unsure about a section, you’ll have time to get help.

SUN DOG

CYBER INSURANCE IS A BREEZE WITH A STRATEGIC IT PARTNER

A QUICK REFERENCE GUIDE

THE CYBERSECURITY CONTROLS TRAFFIC LIGHT SYSTEM

Now that you know some of the key terms you will see on your insurance application, let's get into some **common requirements** you will see within those applications. In the table below, we will start with the baseline requirements to qualify for insurance, then work our way to best-in-class recommendations that may help lower your insurance costs.

RED

Minimum Standard
of Security Required

Failure to implement these practices will exclude you from coverage.
Super important. Vital.

- MFA for employee email access on a non-owned/managed device
- MFA for remote access (VPN) and remote desktop protocol (RDP)
- MFA for privileged accounts/privileged access
- Offsite, and preferable online, backups of critical data
  - Less than 7 days for most data, 30 days for critical, tested quarterly
- Deploy an Endpoint Detection and Response solution on every managed device
- Create a plan for patch management on important hardware and software
  - Demonstrate the ability to apply patches immediately to high-profile programs
- Regular employee cybersecurity training, especially phishing training and simulations

YELLOW

Better Than Red;
Underwriters Love This Stuff

Strict insurers may refuse coverage if you're missing these, especially at big businesses.

- Tracking phishing training simulations
- Robust email filtering tools that block malicious attachments, suspicious files, and more
- Advanced Privileged Access Management applications
- Advanced plans to take unsupported software and hardware offline with plans to fully decommission
- Response and recovery plan, tested and updated
- Block local administrator accounts on managed endpoints

GREEN

Requirements Above Both;
Best Case for Underwriters

All above and beyond necessary requirements, so this is more to help with cost and security.

- Password management through a vault or randomizer with limited access and check-in/out
- Details for service accounts with domain credentials, what they do, and how they are monitored as they move around the network
- Invest in a security information and event management (SIEM) system that offers real-time monitoring and analysis of events
  - Also tracks and logs security data for compliance and auditing purposes
- Invest in a Data Loss Prevention tool that detects and prevents data breaches
- Follow all information security framework available
- Maintain a 24/7 security operations center (SOC)