****

**What is your Cyber Liability?**

3 Things to consider if Cyber Insurance is right for Business Owners

**What is Cyber Insurance**

* History:
	+ They have been around since the 1990s, but did not get attention until recent years
	+ Gone from small intrusions to large scale burglary and theft

**Types of Cyber Insurance**

* 1st Party Risk – Loss or damage to your own data
	+ Ex. Your data is in your data center and it is exposed
	+ If it is just, you…well that will be very rare because there are so many connected to your network
* Third Party Risk – liability to clients, government and regulatory entities
	+ Ex: SAP was hacked and your information along with any partners was exposed
	+ Most cyber policies offer a combination of traditional liability coverage –Protection against claims by third parties

**Number One: What is Covered?**

* Privacy Liability Coverage
	+ Breaches private information which can be a major component of liability
	+ Look for language that states insured “failure to protect confidential information, regardless of the cause
		- Avoid
* Regulatory Actions
	+ High variances on if they will cover for regulatory and other governmental actions
	+ Some policies may require a formal “Suit” that must be filed before coverage
	+ Civil fines and penalties have been covered under many cyber policies and should be mindul if the insurer seeks to exclude this coverage
* Notification Costs
	+ Costs associated with notifying third parties potentially affected by the breach
* Why is this important?
	+ Becoming a priority for third parties to even operate
		- Riders are becoming a requirement on many new contracts
		- Target Breach – HVAC as an example
	+ Could help to reduce judgment if you are doing the right things
		- Security – Check
		- Insurance – Check
		- Good to Go – Maybe!

**Number Two: Premiums – Are they a premium?**

* Can be reduced substantially if you have respectable security practices
	+ What does this mean? Could it be in the eye of the beholder?
	+ Look for Best Security Practices for your business
		- Manufacturing, Financial, etc.….
		- Most are the same but there are some nuances
* Most polices now require that the policy can only be taken out if the client proves they have met the “minimum required security practices”
	+ This is back to point number one…..need to have good practices.
	+ Do you know what this looks like?
	+ Can you get information from a security professional on what that looks like so that you can get it implemented into your environment?
* Fluctuate wildly with breaking news hitting the streets
	+ Example: Anthem breach…..premiums went up as much as 40%
	+ Costs can be a factor so you need to decide on when to buy
* Prices can be negotiable
	+ Don’t be afraid to ask about pricing…all they can do is say no.
	+ Also, in many cases crazy terms/words are used(Breach, Incident Response, Disaster, Intellectual Property Protection, etc.
* **Potential Costs** – These can quickly go beyond lawsuits and regulatory penalties
	+ Incident Response / Crisis Management Team(s)
	+ Forensics Experts
	+ Specific legal counsel
	+ New IT equipment
	+ Public Relations
	+ Credit Monitoring
	+ Reputational losses

**Number Three - Minimum Security Practices**

* Can be defined by you, but should closely resemble industry best practices
	+ Passwords, Admin Accounts, E-mail Spam protections, etc.
	+ Do you have these defined, and do you even know what they are?
* Secure network design
* Good hiring and exiting process with regards to access to server
* Data encryption, secure connections, etc..
* Use known Standards
	+ National Institute of Standards (NIST)
	+ ISO 27001
	+ Others….
* In reality…it pretty much a placebo…but it does force companies to at least consider cyber securit

Other [key](http://www.darkreading.com/perimeter/how-cookie-cutter-cyber-insurance-falls-short/a/d-id/1316365?_mc=RSS_DR_EDT) areas to consider researching cyber insurance

* **Terms and Conditions** – Watch these and they may have significant impact on available coveage
* No standard form on which the insurance industry as a whole underwrites cyber coverage
* **Exclusions** – These are the primary [exclusions](http://www.csoonline.com/article/2835274/cyber-attacks-espionage/cyber-insurance-worth-it-but-beware-of-the-exclusions.html) and your policy could have all or some depending up your carrier.
	+ Cyber-Terrorism – I would have them define what that actually means, especially in the wake of the recent hacks against Sony, Home Depot, etc..
	+ Intellectual Property (IP) Stolen – This is such a subjective part and thus they not are willing to cover your specific IP.
	+ Paper Files – Some insurance companies may not allow cover any information that is within paper documents
	+ Claims by Government/Regulators – This could affect fines or defense cost coverage which would leave a gap
	+ 3rd Party Data – If you entrust data with a third party vendor (Cloud, HVAC, anyone really) there is a possibility it may not be covered
	+ Encryption – The policy may be void if you did not use encryption with your data, which in reality truly complicates matters
	+ Negligence – The failure by the business to install software updates or security patches. This could cause you just as much complications as the above bullet on encryption.
* **Discovery** – In most cases, it takes weeks, months or even sometimes years before it has been discovered disclosed
* **Accidental Disclosure** – If this occurs through yours or an employee’s inadvertent action, the resulting damage can be just as damaging as a hacker stealing your data

**Bottom-line:**  Cyber Insurance can help with reducing or transferring your overall liability risk by offsetting your financial losses but the fine print needs to be completely understood.