PROTECTING YOUR DEALERSHIP FROM CYBER LOSSES

Welcome to the 21st century crime wave

Cybercrime is one of the most talked about subjects facing businesses today. Unfortunately, it is also one of the most misunderstood and avoided subjects. Lengthy articles full of jargon and buzz words and hard to understand information can be confusing for many of us. Besides, we are in the business of selling cars and we don't typically have sophisticated computer systems, how does this really impact our business?

When we talk about Cyber Risks, we are really talking about protecting yourself and your business from a type of 'Crime'.

Technology has increased tremendously over the last couple decades, changing the way we shop, bank, or make travel arrangements. Things are simply *different* now, especially considering the global issues facing all of us. Our dependence on this technology exposes all businesses to what is called a *Cyber Attack.*

More than ever we send things electronically rather than by mail. We bank online rather than in person. Data, including our customer's personal data, is scanned and stored electronically potentially making these records available to anyone, anywhere, anytime.

Incidents of cybercrimes have doubled in the last five years and, given our continued developments and dependence on technology, it is not going away.

Fortunately, insurance companies have created what is called a 'Cyber Insurance Policy' that provides insurance coverage for these types of attacks.

Before we discuss cyber insurance let us look at a few cyber incident scenarios.

Electronic theft of your assets. A cyber criminal simply transfers your funds using social engineering scams. A common scenario is when the bank calls to let you know there has been suspicious activity, most commonly a questionable wire transfer, on your account. The bank 'rep' (who is actually a cybercriminal) requires you to provide your log in and password so they can investigate the matter. The business owner or bookkeeper provides this information hoping to stop the problem immediately. Once this information is provided the cybercriminal will initiate transfers from the account. When we hear of such a scam it is easy to judge the scenario and say "that wouldn't happen to me" however the surprise of hearing the account has been hacked combined with the skills of the cybercriminal often catches us off guard.

From the banks point of view, if it is determined negligence on part of the business allowed the criminal activity the bank is *not* obligated to cover your loss. To prevent such losses, you need to be aware of the changing techniques these cyber criminals are using. This is difficult enough for people who understand the changing technology, but what about the rest of us? Where do we even begin to look?

Extortion is the fastest growing area of cybercrime. The cybercriminal takes control of your digital assets, holding them for ransom. These criminals use what is called ransomware to take control of your files. You will not be able to access files, or worse, if you do access them the ransomware begins to destroy those files. Business owners have a choice, succumb to the extortion, and pay the ransom or

see their business grind to a complete halt with systems and data destroyed requiring costly repairs, if that's even possible!.

Theft of your data- data is key to a cyber criminal's success. Identity theft rings need as much data as they can get and are willing to pay handsomely for it. A cybercriminal will steal this data from your files with the intent to sell it. A simple list of names and addresses will sell for more than you may think. Imagine the value attached to a dealer's data which often includes social security numbers, driver's license, copies of checks, credit applications, and auto registration information. Once this data has been breached your customers are now at risk and they are looking to you for reimbursement.

Business Reputation- if an incident or breach occurs involving your customers you will need to inform them. Such an incident damages the reputation of the dealership, shaking confidence, and reduces the likelihood of a repeat customer. We all know it cost much less to prospect a repeat customer than to find a new one.

A cyber insurance policy can pick up the costs involved in responding to a cyber crime including IT security, forensic specialist support, the cost of notifying individuals that have had their data stolen and providing legal support. Most importantly it can provide access to the right specialists and cover the costs related to these services.

A cyber policy can also cover the costs to repair and rebuild lost data and damages causes to computer systems in the event of a cyber incident and cover the costs to rebuild your reputation online.

Other valuable coverages include *business interruption coverage* caused by a cyber incident. Like business interruption coverage often found in a property policy, cyber insurance business interruption will help cover the costs necessary to rebuild your data and systems and additional labor needed as you work through the process.

Think your business is too small to suffer a cyber-attack? Think again. A recent Verizon Data Breach Investigation report showed that 58% of all cyber-attacks involved small business. In fact, cybercrime is now so common it is no longer newsworthy when a small business is attacked, we only hear about the big ones!

With most bank lobbies closed due to current restrictions we are all forced to bank differently, using electronic transfers and 'trusting the system'. This exposure is greater than ever.

Protecting data in todays world is difficult. Even if you are using a third-party cloud service or if you have invested in strong IT security controls, with changing technology you can never be 100% certain you will not be exposed.

Cyber Insurance is *not* typically part of your dealership garage policy and not all policies are available to dealer operations. A stand-alone cyber insurance policy will cover the gaps and exposures alongside your garage policy and some policies provide access to expert cyber claims handlers and a wide range of technical specialists.

As with any policy there is a cost associated to purchase cyber insurance although it is often quite affordable and certainly better than exposing your business to a loss of thousands if not hundreds of thousands in uncovered losses. Contact your insurance agent and ask if he or she has access to a stand-alone Cyber Insurance Policy suitable for auto dealerships.

Todd Shepard is the founder of Shepard & Shepard Insurance and regular contributor to the Front Row.

For more information or an affordable quote on Cyber Insurance for your dealership call toll free 855-396-0488