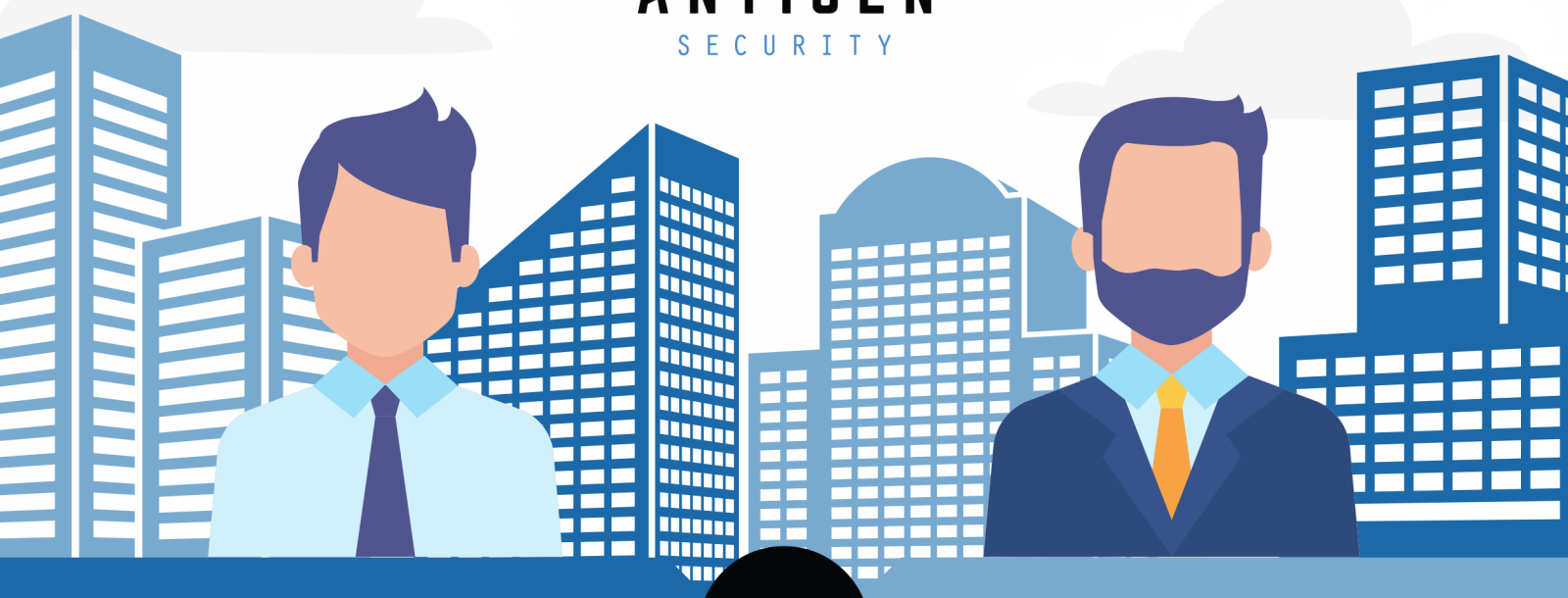
ANTIGEN
SECURITY



Unprepared Biz VS Biz + IR Planning

Unprepared Biz		Biz + IR Planning
Your business experiences a cyber attack and begins to panic. You immediately turn to your attorney and insurance company on the next business day.		Your business experiences a cyber attack and rests easier knowing you have a plan. You contact your dedicated Incident Response team via 24/7/365 hotline.
The insurance company assigns their own Incident Response team who begins work with no previous knowledge of your IT environment resulting in significant excess expenses.		Your dedicated IR team has an understanding of your IT environment and is already aligned and approved by your insurance carrier, saving you considerable time and money.
The 3rd party IR team assigned by your insurance company and attorney start billing you per hour, while your own IT team pours out assistance costing you even more.		Your dedicated IR team provides high/low estimates and reduced pricing for a compromise assessment. You are able to better budget for your investigation (or use a prepaid retainer).
The insurance company and attorney are incentivized to “place blame” for the incident, which undoubtedly falls on either your own IT team or your affiliated Managed Service Provider.		Our IR team is able to determine the actual date of entry, real source of the breach and begin to remediate the situation and help restore your environment.
You begin to question why this incident happened and realize that you didn’t plan properly, which is going to cost your company significantly.		Your entire company is relieved knowing that you were prepared with proper IR planning and a dedicated team that reduced the timeline and cost related to recovery.
The 3rd party IR team, insurance company and attorney order your company to purchase a litany of cyber security controls from yet another 3rd party.		Your company is able to implement only those additional cyber security controls necessary to enhance security and further protect yourself from future events.
You begin paying your bills and preparing to defend yourself against any potential D&O or subrogation claims that could arise from your affiliates, partners, customers.		You have successfully contained a cyber attack and have your business back up and running in a reasonable time with no extraordinary expenses or additional outside risk.