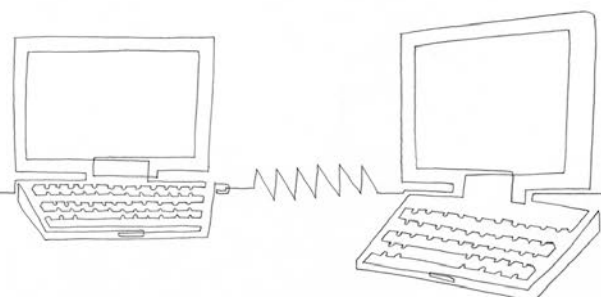


## Overcoming Buyer Objections

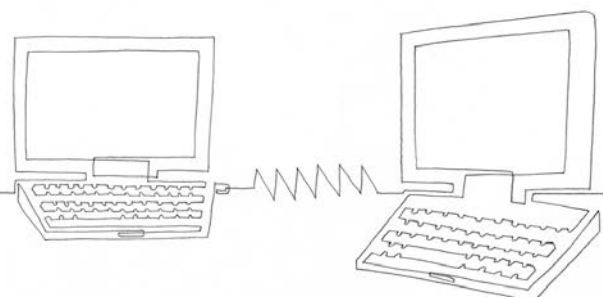
Objection	Response
My <XYZ> policy has a \$25,000 sublimit for data breach expenses.	<p>The client should consider if: 1) the sublimit is adequate given the likely costs that will be incurred; and 2) if the sublimited coverage will apply to all of the costs that the entity is likely to face (notification, computer forensic services, defense of claims made against the organization).</p> <p>The client should also consider the value provided by the assistance provided in connection with a dedicated data breach response policy. In all likelihood, the entity does not have significant experience with handling and responding to data breach incidents and issues. A significant part of the value of a Beazley Breach Response (BBR) policy is the assistance provided by the BBR Services team.</p>
I have data breach coverage in a commercial general liability policy.	Data is not tangible property and property damage coverage does not extend to damage to intangible property. The commercial general liability policy wording has been revised to specifically exclude data breaches.
We're not a retailer, hospital or bank. We don't have any exposure to this type of loss.	<p>All entities have some exposure. Ask the following questions:</p> <p>Do you maintain personally identifiable information about employees?</p> <p>Do you sign non-disclosure agreements or hold confidential business information of others?</p> <p>Are you concerned with a loss of income or extra expenses from a disruption to computer services?</p>
We don't handle, process or store credit or debit card data.	This may be true, but the entity may process and/or handle card data without fully realizing it. The entity should carefully review the terms of the Merchant Services Contract they signed in order to accept payment card payments. Most agreements require the entity to obtain a computer forensic audit upon the demand if any of the payment card brands suspect a breach has occurred, as well as for the costs of card re-issuance and card fraud losses resulting from a breach.
Our CIO says our systems are completely locked down and don't need coverage.	There are two points to consider: 1) The science of risk management says that for every exposure to loss a firm should have, at least, one form of risk control and at least one form of risk financing, because no set of risk controls can guarantee that an entity will not have a list; 2) the entity should also be aware that many losses result from things outside the control of the IT department. 18% of losses result from a physical loss of records; 30% occur as a result of a loss of information in the care of a vendor and 24% of breach events occur as a result of a broken business practice.



## Overcoming Buyer Objections

Objection	Response
We're not Target stores, nor are we a likely prospect for a cyber attack	<p>We hear about mega breaches in the media, but the vast majority of breaches are small (&lt; 100,000 records) and relatively boring to the media (unless they happen to you).</p> <p>Also, not all breaches are electronic in nature. 18% are physical loss. More and more middle market and small businesses are suffering cyber attacks; frequently in the form of ransomware. A cyber attack may also be targeted at a vendor of the suffered entity.</p>
We won't need assistance with computer forensics. Our information technology staff know our system the best.	<p>To maintain the best defensible position for a claim/suit seeking damages or even a regulatory investigation, the best practice is to conduct an outside, impartial, 3rd party investigation.</p> <p>Furthermore having privacy counsel retain a third party computer forensic firm may help bar discovery of unflattering information not directly related to the claim.</p>
We can handle a breach with our internal staff.	<p>State security breach notification laws are complex. The laws apply based on the location of the consumer not the location of the business.</p> <p>Government regulators may be difficult to deal with. There may be "unwritten rules" or expectations. There is a tangible benefit to working with privacy counsel that has an ongoing working relationship with regulators.</p> <p>The best interests of the organization may involve an investigation lead by privacy counsel and utilizing outside resources to avoid claims of a cover-up.</p>
We don't want to be forced to use panel firms for a breach event.	<p>Large firms with significant expertise handling breach events may be in a good position to handle a breach. In this case, Beazley can offer coverage via the Beazley Information and Security Liability Policy form.</p> <p>Smaller firms will benefit from the expertise and assistance of the BBR Services team, as well as high quality firms for breach response services.</p> <p>Amongst other benefits, Beazley can arrange services when capacity may be thin due to unrelated events and has negotiated significant discounts to normal rates for services.</p>

beazley



## Overcoming Buyer Objections

Objection	Response
We want to use our normal outside counsel, and not one of the panel firms required under the BBR policy.	<p>Privacy (data breach) is a legal speciality, and Beazley is proud to have expert privacy counsel as a part of the panel for legal services. Other counsel may need to research issues that panel counsel have litigated or researched in the past. Furthermore, Beazley panel counsel have negotiated lower rates for services.</p> <p>The purpose of the Beazley panel is to obtain the best and most efficient response for the insured entity.</p>
Every carrier handles claims the same. There's no difference between carriers	<p>Beazley offers the services of a dedicated in-house BBR Services team. The BBR Services team is separate from and distinct from the Beazley claims team, and is solely focused on assisting the insured to resolve an actual or suspected breach event as quickly and efficiently as possible.</p> <p>The Beazley claims team, on the other hand, is responsible for confirming that coverage applies and for making claim payments.</p> <p>We are unaware of any other insurer offering an internal breach response services team.</p>
We want to use <<breach facilitation service>> to manage the breach event	<p>There are a number of high quality breach response facilitation firms available in the market. In most cases, these providers do not perform all services in-house and subcontract many aspects of the response to third parties. In our experience, this has resulted in excessive costs, due to unnecessary mark-ups of services obtained from third party services providers, as well as quality problems when subcontractors have subcontracted services.</p> <p>Beazley created the BBR Services team to cut-through and provide high quality services at the lowest possible cost.</p>
It is our business. We don't want Beazley to take over the event.	<p>Beazley offers advice and counsel based on over 6,000 breach events that we have assisted insureds to handle. At every step of the way, the final decision, including the choice of the BBR vendors from the Beazley panel, is left to the insured.</p>

The descriptions contained in this communication are for preliminary informational purposes only. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., and is available on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd's. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: 0G55497). CBEM588\_US\_07/16

beazley

