# *overcoming* objections.

**OBJECTION: "We have an endorsement on our package policy that provides cyber coverage."**

- The coverage provided by these endorsements is inadequate. Liability limits are low, and coverage is limited.
- These endorsements provide expense reimbursement only.
- They typically provide no coverage for data restoration, no Business Interruption coverage, no coverage for regulatory fines and penalties, no coverage for Payment Card Industry (PCI) fines and penalties, no coverage for cyber extortion.

**OBJECTION: "I don't have any exposure."**

- Every business has this exposure. Don't think about it as a tech exposure only. The key is to protect your information, which can be electronic or paper. Every business holds some amount of sensitive data which can include the following:
- Personal identifiable information (PII) such as credit card information, social security numbers, drivers license numbers, banking information, employee information, employment information
- Personal Health Information.
- Third Party Corporate Information of clients.
- You are legally obligated to protect data you collect. State and federal regulations dictate proper handling of private information. If this information is breached, agents must navigate the different laws in 46 states that mandate how victims must be notified.

**OBJECTION: "We spent a lot of money on IT, and our IT department says we have great controls."**

- Hacking is only one cause of data breach. Others include:
- Lost/stolen portable computers or media
- Lost/stolen back-up tapes
- Improper disposal of paper records
- Employee misuse
- Vendor negligence
- Intentional release by rogue employees

**OBJECTION: "We aren't a target for hackers."**

- Data breaches are common among smaller businesses. Some 55 percent of small businesses responding to a recent survey have experienced a data breach, and 53 percent have reported multiple incidents. If you collect sensitive information from policyholders, you are at high risk.
- Data held by small businesses is low hanging fruit... hackers know these enterprises lack the security resources of their larger counterparts. Only 38 percent of breaches in the latest Verizon study impacted larger organizations.

**OBJECTION: "If we have a breach, we will handle it ourselves."**

- Responding to a breach is not only costly – running an estimated $200,000 – it's complex. Experts from multiple disciplines -- from forensic investigators, to public relations firms, to privacy counsel -- may be needed to mount a coordinated response to even a small incident. Botch the response, and your reputation can be irreparably damaged. There is also the specter of regulatory fines and penalties and legal liability.
- A single laptop left on a commuter train or stolen at an airport can cost a company nearly $50,000 – most of that being expenses to respond to data breached – or potentially breached.

**OBJECTION: "We use a 3rd party service to handle our credit card payments and store our data, so it's not our problem."**

- It is not your vendor's responsibility to notify your customers. It is yours. This is a legal requirement that cannot be changed by contract.
- Even if you outsource data handling, your exposure stays in-house. You may feed data into third-party systems or outsource data storage to a cloud provider. Still, if your agency's data is breached, you are legally obligated to respond.
- Some 70 percent of small businesses report that breaches are most likely to occur when outsourcing data.

McGowan, Donnelly & Oberheu, LLC • Phone: 512.600.2280 • www.mdoinsurance.com • 106 E. 6th Street, Suite 520 • Austin, TX 78701

mdo
mcgowan, donnelly & oberheu, llc

*Network Security and Privacy Liability*

# DON'T LET YOUR CLIENTS BECOME A TARGET!

**Network Security and Privacy Liability** are exposures every insured has, yet the vast majority either have no coverage or insufficient coverage. There are dozens of products available, but there is **no other** product on the market like Beazley Breach Response (BBR).

BBR is more than an insurance policy. It is also a loss control and risk mitigation service for the insured. Policyholders gain access to a comprehensive risk management service that features state-specific summaries of privacy & data security laws, compliance forms & procedures, training materials, specialist support, and much more.

## Why Beazley? And why *this* policy?

- BBR offers notification provided on a number of affected individuals basis, not a capped dollar amount. Notification is provided outside and in addition to the limit of liability.

- Beazley is the only carrier with an in-house breach response team, separate from the claims department, staffed by breach response experts who have handled over 1,000 breaches.

- Beazley's Breach Response team serves as the insured's "breach quarterback" in the event of a breach. Beazley coordinates the process from start to finish and pays the vendors on behalf of the insured.

## Why MDO for BBR?

- MDO has In-House Quote Authority for the BBR product. Our brokers have the BBR rating tool on their desktop, so they can offer indications very quickly.

- MDO can quote with limited information. We only need the following to offer an indication:
    - Address
    - Revenue
    - Nature of Operations

- MDO can provide same day turnaround for submissions received before 2pm. Our brokers are committed to getting indications to you as quickly as possible.

- MDO can quote from a competitor's application. Our brokers can gather the information needed to indicate from any application.

## Contact me for additional information:

McGowan, Donnelly & Oberheu, LLC • Phone: 512.600.2280 • www.mdoinsurance.com • 106 E. 6th Street, Suite 520 • Austin, TX 78701