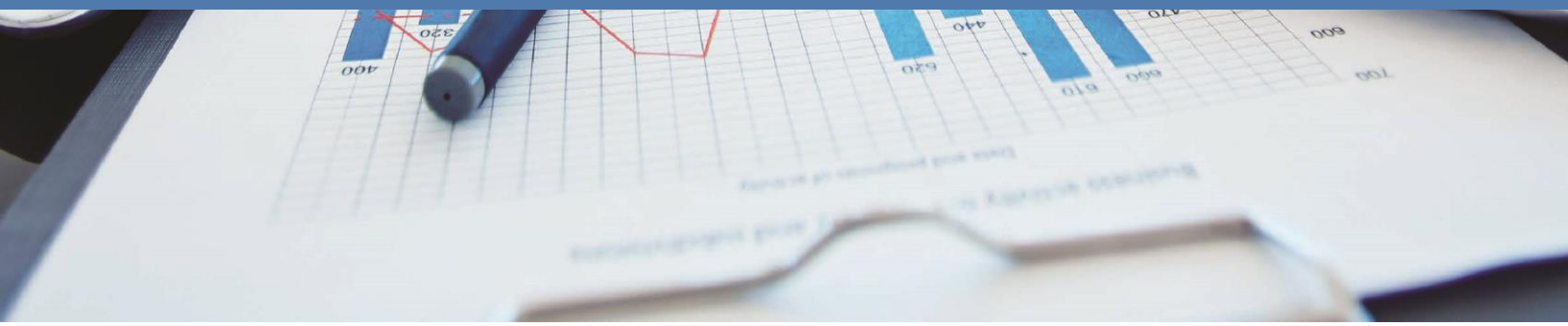
CYBERCRIME:
BAD NEWS FOR MIDSIZE FIRMS



Multipoint NETWORK

"The Point is Service - **Fast**, Reliable I.T. Services"

CYBERCRIME: BAD NEWS FOR MIDSIZE FIRMS

Two of the topmost concerns that appear in surveys of CIOs are cybercrime and data security. Rightly so. Nothing strikes closer to the heart of any client than the security of their data. No matter how excellent your product or service, if your clients feel their data is at risk, they are likely to go elsewhere. This fact is of special concern to medium and smaller sized businesses for two important reasons. First, smaller firms are the most likely targets of cyberattacks, and second, customers are harsher in their response to data breaches at smaller firms than they are about attacks on large corporations.

Let's look first at the likelihood of attack. If you are a small business, then you are a strong target for cyber criminals. Last year, 71% of small to medium size businesses were the victims of cyber-attacks. We hear on the news about big cyber-attacks on large corporations, healthcare conglomerates, as well as government agencies. The trouble with this news coverage is that it creates a distorted view of where cyber-attacks are taking place. These attacks are not solely hitting large organizations and being small by no means keeps you immune. Smaller firms represent a significant portion of those who suffer from cyber-attacks. In fact, small firms can be used as conduits to larger organizations. Smaller businesses have become vulnerable because they are often the inroad to larger, better protected entities. They may be sub-contracting as a vendor, supplier or service

provider to a larger organization. That is likely what happened in the case of the Target Corporation in 2013, when over 40 million accounts were accessed.

What makes this even more serious is that smaller firms are less likely to be prepared to handle an attack. 31% of small to medium sized businesses do not have a plan of action for responding to IT security breaches, and 22% admit that they lack the expertise to make such a plan.

Research has found that customers affected by security breaches are generally less forgiving of smaller businesses, especially smaller online retailers, than larger companies. As a result, medium and smaller firms not only must contend with absorbing lost revenue and expenses, they also face a greater possibility of never regaining the customer's trust.

What does all of this mean? Firms need to prove they are on top of their infrastructure's security, or risk losing customers and not winning contracts with large businesses. CIOs need to keep on top of all the strategies available to protect their infrastructure. CIOs of large firms are deeply aware of this, but smaller businesses remain less likely to focus resources on anything not directly related to revenue production. Too often, this means less IT security investment. However, this is an area where you cannot afford to cut costs because the consequences are too critical for your business's future.

For Additional Information Please Contact

Brian Bloom | Email: brian@mpn1.com

Phone: (310) 499-0169

315 North Crescent Drive, Beverly Hills, CA 90210