



How to Keep Price From Becoming an Object

WHEN THE NATION BEGINS TO WORK ITS WAY OUT OF THE COVID19-INDUCED RECESSION, WE SHOULD ALL REMEMBER THAT PEOPLE DO NOT MAKE BUYING DECISIONS BASED SOLELY ON PRICE.

Price is a factor, though. If a prospective buyer sees no qualitative difference between your product or service that costs \$100 and a competitor's product or service that costs \$75, the competitor will be the likely winner. Marketing guru Ray Jutkins taught me a lot about what matters to prospective buyers.

"Price is not a value!" Ray said. Surveys routinely show that price is not an issue when extreme value is offered. That means it's important to understand what your customers want. You've doubtless noticed that prices are higher at convenience stores than at grocery stores. The customers value convenience and are willing to pay more to get it even though the stores often have less than stellar services and limited selections.

Ray explained that competing on price alone is almost always a failing strategy. Instead of educating prospects and customers about value, companies that do this talk about how cheap they are.

Don't Be Cheap

IF PRICE ISN'T A BENEFIT, THEN "CHEAP" IS DEFINITELY NOT A BENEFIT. WHO WANTS CHEAP?

Inexpensive, maybe; but not *cheap*. A company that sells "cheap" cultivates cheap customers. That leads to other problems as the company keeps wages low and may cut corners on production.

Underpaid workers are rarely delighted to come to work each day and their dissatisfaction transfers to customers. Customer loyalty falls victim to poor employee attitudes, shoddy products, and mismanaged services.



The Customer Comes Second, a book by Hal Rosenbluth and Diane Peters, shows why *the customer comes first* is the wrong approach for a business to adopt. Treat employees poorly and they will treat customers poorly. Rosenbluth and Peters tell managers to encourage their people to treat one another like clients. One goal is to eliminate the *us-versus-them* attitude that can occur in any organization because this attitude then grows to an *us-versus-them* attitude regarding customers.

The Value of Value

CONCENTRATING ON VALUE INSTEAD OF PRICE AND MAKING SURE THAT EMPLOYEES ARE TREATED WELL WILL HELP AS WE BEGIN TO RECOVER FROM A BADLY DAMAGED ECONOMY.

Value includes aiming for perfection. That's an unattainable goal, but a worthy one. The *Merriam-Webster Unabridged Dictionary* contains more than 263,000 main entries. If the dictionary editors spelled 99.9% of the entries right, 263 head entries would be wrong.

United Parcel Service delivers nearly 22 million packages and documents every day. If they correctly deliver 99.9% of those packages, there would be 22,000 misdelivered packages every weekday. Oh, and if UPS pilots landed 99.9% of the company's planes properly, eight UPS planes would crash every week.

The battle to regain customers will be arduous. The expectations will be for superior service, accuracy, quality, and cost. So price is a factor, but it is not the most important factor.

Avoid the temptation to drop prices the instant a prospect voices an objection. Returning to Ray Jutkins for a moment, his advice was always to understand what the prospect was really asking – objections, he said, are almost always requests for justification. Why should I buy this product or service? Why are you the best supplier?

Answer those questions and price fades into the background. 🏹

Working From Home Exposes Security Issues

RESEARCH THAT SHOWS COMPANY SECURITY IS MORE AT RISK WHEN EMPLOYEES WORK FROM HOME

IS LIKELY TO BE THE LEAST SURPRISING NEWS ANY CHIEF SECURITY OFFICER (CSO) HAS EVER HEARD.

NOT EVERY ORGANIZATION HAS A CSO AND THOSE THAT DON'T ARE EVEN MORE VULNERABLE.

Network security rating company BitSight says it has found significant security issues across the rapidly rising number of networks used to work from home. The researchers analyzed more than forty-one thousand organizations and BitSight says many companies suddenly face newly exposed or vulnerable devices and services because of malware-infected networks.

I spent several years working in an office for a company that handled a sizable amount of data from the United States and Canada. My desk was adjacent to the chief security officer for a time, so I gained some insight into the issues he faced. I had a home office for the final few years that I worked for the company and appreciated the end-to-end security the company used.

Encryption and Surveillance

WHEN I HAD TO WORK WITH CLIENT DATA, IT CAME TO THE COMPANY-OWNED COMPUTER ON MY DESK FROM THE COMPANY'S SERVER.

Data was encrypted on the server, during transmission across the internet, and (except for when I was actively looking at it) on the computer's disk drive. Everything was encrypted all the time, but that's only part of the issue.

Social engineering, phishing, and other threats can get through to workers when they're at home. Many companies have started using applications that work with the corporate email system to clearly mark all messages that originate outside the corporate network. But crooks will be crooks and no matter what protections are in place, the crooks will poke around until they find a way to defeat them.

BitSight recently released a work-from-home remote office application that allows organizations to monitor security in remote offices and on networks. The system differ-



A WORKER'S DOG MIGHT EAT AN IMPORTANT REPORT OR A CAT MIGHT OVERTURN A GLASS OF WATER ONTO A COMPUTER, BUT MUCH MORE SERIOUS THREATS MAY EXIST ON THE HOME NETWORK THAT CONNECTS THE EMPLOYEE TO THE CORPORATE NETWORK.

more distinct families of malware present than the corporate network.

Although 17% of companies had at least five distinct malware families on their employees' work-from-home networks, slightly more than 2% of companies had that level of infestation on their corporate networks.

Well-known botnets — networks of computers infected with malware — are more prevalent on work-from-home networks.


Home networks expose the corporate network to vulnerable services and devices. Cable modems, routers, cameras, storage peripherals, and other internet of things devices are found on home networks and many of these devices fail even simple security tests.

Addressing New Challenges

BITSIGHT SAYS MORE THAN A QUARTER OF WORK-FROM-HOME NETWORKS HAVE ONE OR MORE SERVICES EXPOSED TO THE INTERNET.

Six in ten have an exposed cable modem control interface, a flaw that is one of the most popular targets attacked by crooks.

BitSight's Chief Technology Officer, Stephen Boyer, says that a company's security risks rise sharply as a massive workforce suddenly accesses sensitive resources from outside the corporate network. "Addressing cyber risk to the remote workforce has become the primary concern for security and risk professionals."

BitSight's report, *Identifying Unique Risks of Work-from-home Remote Office Networks* is available on the [company's website](#). 

entiates between corporate networks that are typically behind several layers of protection and work-from-home and remote-office (WFH-RO) networks.

Malware on Home Networks

BITSIGHT GAINED VISIBILITY INTO THE OPERATIONS OF REMOTE NETWORKS AND FOUND THAT THE SURGE IN WORK-FROM-HOME ACTIVITY HAS "DRAMATICALLY EXPANDED THE CYBERATTACK SURFACE IN WAYS THAT MAKE COMPANIES AND THEIR DATA VULNERABLE." THE RESULTS ARE TROUBLING.



Networks that connect work-from-home employees to the corporate network are over three times more likely to have malware present than the traditional corporate network. Malware was found on 45% employees' work-from-home networks, but on "only" 13% of corporate networks. The fact that so many corporate networks have malware is disturbing in its own right.

BitSight says these home networks are nearly eight times more likely to have five or