How to Sell Security

July 2013

CONTENTS

EXECUTIVE SUMMARY 2
ADDRESSING THE CHALLENGE 3
WHAT IS SECURITY? 4
THE PLAYERS IN THE SALES PROCESS 5
- Executive / Enterprise Sales 5
- 'Other' Sales 5
- Sales Engineers 5
- Subject Matter Experts 6
- New Sales vs. Account Management 6
- Sales Operations 6

PREREQUISITES 7
- Vision & Values 7
- Methodology 7
- Consulting Wrappers 8
- Patience 8
- Courage 8

THE PROCESS 9
- Phase I - Opportunity 9
- Phase II - Delivery 9
- Phase III - On-Going Account Management 9

WHAT TO SELL, WHEN, AND WHY 10
- Phase I – Education 10
- Phase II – Risk Assessment 11
- Phase III – Control Gap Analysis / Health Check 11
- Phase IV – Remediation Guidance & Control Definition 12

SELLING TO THE VALUE NOT THE COST 13
SUMMARY 14
ABOUT FROUD 15
ABOUT CORE CONCEPT SECURITY 15

EXECUTIVE SUMMARY

This white paper is not about *how* to sell, I am not a salesperson, but I have a lot of respect for those who do it well.

Unfortunately, there are those who leave a lot to be desired, and these concepts will be difficult to implement for anyone who meets any of the following criteria:

- Only cares about making money, and will do so without regard for anyone else;
- Doesn't have the patience to build a pipe-line over at least one year;
- Works for a company with neither vision nor appropriate values; and
- Integrity is not a core personal value

The more cynical readers will say that this would include all salespeople, but that is simply not true. I have met many salesmen and saleswomen who truly understand the importance of what security professionals and business owners the world over are trying to achieve, buy into that vision, and want to help. And make money of course.

But just as poor consultants ruin it for the profession, poor salesmanship taints the market to the point where – if we're not careful – we'll be seen as selling snake oil. The struggle to sell what amounts to a decades old concept; security done properly, becomes a drive for the next 'silver bullet' solution, or worse, a single end-point product.

There are only so many ways you can explain what security is, until even the critical aspects of it start to appear meaningless. For example, a Risk Assessment is perhaps the most important step at the beginning of the implementation of an overarching, business enabling, security framework. But try selling one.

Instead, if you throw out phrases and buzz-words like, The Cloud, Artificial Intelligence, Machine Learning, and GRC, and suddenly you have everyone's attention. The market (i.e. security vendors) has created the need, just like Apple did with their iPhone. While I realise that the sales department is always under pressure to make quota, you cannot be in this for anything other than the long haul.

The following pages will break down my thoughts on everything from what security is, the type of salesperson(s) required, the sales process itself, and how it all fits together into a process any security organisation can follow.

As I've said many times in my career; Security is not easy, but it CAN be simple. The sales process is equally simple, and every bit as difficult to do well.

Finally, this document is designed to not only help you, the salesperson, make it in this increasingly competitive space, but it's also for those BUYING security services, as that side can be equally difficult to get right.

ADDRESSING THE CHALLENGE

As unfortunate as it is, selling security is like selling insurance; no-one WANTS to spend money for no obvious return on investment (ROI), but know they have to for any number of reasons; law, risk transfer, liability protection, you name it.

This means *buying* security is seen only as an expense, and as a tick-in-the-box[1] exercise to be delegated to the lowest bidder. Combine this with the fact that most IT, and especially IT Security, departments are seen as a roadblock to business growth and not enablers, and the concept of a 'business-goals oriented' security program rapidly falls apart.

Another negative aspect of these perceptions is that as a salesperson, you're rarely going to have the opportunity to talk to the people who hold the purse strings. You will be talking to their designate, or worse, a designate OF a designate, and there is a fairly good chance neither of them cares. Strangely enough, even if they DO work in IT, security is often seen as another burden on top of their primary function of keeping things running.

Getting management buy-in, while difficult, is not even the first problem you'll encounter; it's finding the right business drivers to get in the door in the first place. These drivers are increasing, most notably around personal privacy issues, but for a while there it was only the Payment Card Industry (PCI) that had people's attention globally (the US had HIPAA too).

Unfortunately, because the PCI DSS a) is just about credit cards, b) is mostly just a bunch of controls, and c) was both introduced and managed badly, it was not really taken seriously, and certainly not seen as something these organisations SHOULD have been doing in the first place. Which it most certainly is.

Consequently, the audit / tick-in-the-box approach taken by a large number of 'Just QSAs' companies, some of whom have the nerve to call themselves 'Trusted Advisors', has left a rather bitter taste in the mouths of their clients. Especially if the client ended up buying a bunch of products from the same company, just to discover that they don't provide any benefit to the rest of the business, or in some cases, even in the one place where they should.

The final challenge – for the sake of this white paper anyway – is that most salespeople are not security experts, and unless they have at least a reasonable background in what security is, having the right conversations with the right people is very difficult.

All of these issues will be addressed throughout this document.

WHAT IS SECURITY?

Throughout this document I will use the phrases 'security program', or 'security done properly', or words to that effect. In each case, I refer to the table below. You will notice that of the standards / compliance regimes I have mentioned, not one of them covers all requirements. Nor can it.

True security, one that enables the business, is a series of never-ending processes all with one goal in mind; keeping the business running responsibly and successfully.

This is not something you sell up-front, it's something that develops over time, and ONLY when you have earned the role of Trusted Advisor can you provide it. Until you are helping them reach their business goals through an effective security program, you are just a consultant.

At a very high level, a security program will contain all of the following steps;

Security Program Elements	PCI	ISO	COBIT	SGP*
Review Business Plan / Goals			✓	✓
Risk Assessment	✓	✓		✓
Business Impact Analysis		✓		✓
Policy & Procedure Formalisation	✓	✓	✓	✓
Security Control Implementation	✓			✓
Management Systems Implementation		✓		✓
Hand-off to Governance Committee			✓	✓
Change Control Integration	✓	✓		✓
Disaster Recovery & Business Continuity		✓		✓
Initiate Information Security Life Cycle**		✓	✓	✓
Begin Business As Usual				✓

* Security Good Practices ** Plan > Do > Check > Act > Repeat

The first step as a salesperson is to learn enough about these concepts to ask the client the right questions for you to then know whom to bring to the table to continue the process on your behalf.

Unless you are one of those VERY rare people who is both a security expert, AND a first-class salesperson, it's not your job to explain security to the client, it's for you to know the people who can.

Never sell a client what they ask for, unless they truly know what they need.

THE PLAYERS IN THE SALES PROCESS

The sales process in security is a little more complex than most, as you are talking about something that can have an enormous impact on the performance of the client's day-to-day business. It's also a little a longer process than most, because it's very difficult for the client to see the value of what you're selling when; a) they probably don't want to buy it in the first place, and b) security done properly is not always cheap and you will always be underbid.

But this raises one of the most important aspects of selling security: Selling to the value, not the cost. This will be handled in its own section.

The players are:

Executive / Enterprise Sales

These are the folks who really understand people, and are able to cut through the majority of the purchasing red tape and talk directly to the ultimate decision makers. They instinctively understand that the higher they can make it up in the organisation's food chain, the more influence they'll have on all layers beneath.

Executive sales are often seen as slick, glib, or other fairly unflattering adjectives, but the *right* executive sales people are very well respected, and have significant connections in the upper management levels in many industry sectors.

They are not cheap, but critical if you want the access to the big players, and the big deals.

'Other' Sales

This is meant as no disrespect to anyone not in Executive Sales, the other forms of sales are every bit as important, it's just that there are so many titles for them that it's best to be general.

These are the folks that do anything from small businesses, to telephone sales, to focusing on specific sectors. They will generally have more and smaller clients, and probably do more business on the phone than they do in person.

Regardless of the differences in scale, the sales process is the same.

Sales Engineers

In some organisations these guys don't get anywhere near the credit they are due, in others way too much, but either way, if you are trying to sell ANY kind of product, you'd better have a few.

Generally speaking, they are the rare-ish breed of folks who are deeply technical, yet can be put in front of clients without worrying about the result. In effect, they can translate what the salesperson is trying to say into geek-speak for the client's technical team, and into English for the business side.

Some product-only companies ONLY have sales engineers, but without the polish of the enterprise sales, the bigger deals will probably be beyond reach.

Also, unless the sales engineer has deep security consulting experience, using them to sell services is a mistake.

Subject Matter Experts

In the end, it's the subject matter experts (SMEs) that make the sale possible. Whether it's a security consultant, a penetration tester, or some other guru, it's the SMEs that put the conversations the salesperson started into perspective for the client's security program, and hopefully, also their business goals.

The salesperson opens the door, the SME answers the questions, and between the two-man team (or possibly 3), the client has all their questions answered, and concerns laid to rest.

New Sales vs. Account Management

This is one of the few times I will venture into opinion on how the sales department itself should be organised. But it's simply not my area of expertise.

That said, I have always maintained that there are 2 very distinct and separate types of salespeople; the 'Hunters'; and the 'Growers'

> *Hunters* – Very aggressive, easily bored, hate detail, DESPISES paperwork. Basically, these guys want to get in, get the deal signed, and move on to the next battle.
>
> *Growers* – Less aggressive, and tend to prefer to relate to the client on a more personal level. Get to know them. These are the folks who will take the initial sale and turn it into years of upsells / cross-sells though their deepening understanding of a) the client's business b) the client's people, and c) the state of their security program.

In my experience, having every sales rep perform both duties is a big mistake, and neither aspect gets done well. As a result, the client rarely buys everything they would have, customer satisfaction remains low, and the salespeople get frustrated.

Sales Operations

These people *never* get the respect or thanks they deserve, but without them the whole process would fall apart. Sales Operations means different things to different companies, but from my perspective, if they just take care of the 'paperwork' for the sales folks, the salesperson can get on with what they do best, and everyone wins.

It is the combination of ALL of these players that makes selling in security possible; the right skill-sets applied at the right time, to the right people on the client side. Everything else is just scratching the surface.

PREREQUISITES

If we assume that we have the right people on the sales team, there are several factors that if not in place from the beginning, will cause the process to stick, or even fail entirely.

Vision & Values

If the organisation that YOU work for does not have the appropriate visions and values, it will be obvious to your clients from the requests for proposals (RFP) stage onwards. Some companies even include things like that, green policy, and community contributions into their RFPs, so any organisation that has/does none of those things is at an immediate disadvantage.

Your CEO sets the tone for your organisation. If they have no *obvious* values of integrity and customer service, this will be pervasive down to his 'inner circle', then beyond to senior management and so on. An organisation that is not 100% behind a culture in which they can believe, will not be as successful in security as one that does.

Per the first page of this white paper, your OWN vision and values must also have the client's best interests at heart, or again, they will not ring true.

Selling security is not as much about the services you provide, as it is about the relationships you can build.

Methodology

If you're a services-only security company, you have to have a standardised methodology for the delivery of those services, and this must be very well understood by everyone in the sales cycle.

The biggest complaints clients have regarding consulting services of any kind are, in order of importance:

1. *Communication* - This encompasses everything from communicating the initial plan, agreement of the goals, and the on-going communication between all relevant parties. Clients do not get as angry when things go wrong as they do when they are the ones chasing YOU after they *have* gone wrong. The majority of communication in consultancy is pro-active, or at least is should be;
2. *Guidance* - This is what they are paying you for, and if they don't get it, they have every right to be upset. The consultants you provide should have more than enough experience to deliver exactly what was sold, and preferably, just a little bit extra. Clients don't want an auditor, they want someone who can help resolve their challenges. The client should have to ask exactly the right questions, the consultant should already know the answers, or know someone who does;
3. *Consistency* - There is nothing quite like having to tell a client that the £10,000 they spent fixing a compliance issue was not necessary, oh, and by the way, here's how it *should* be fixed;

   Decisions that involve any significant outlay in terms of capital or resource expense should never, repeat *never*, be signed off by an individual. The consulting *company* should sign-off to ensure that all decisions are final regardless of the consultant on the ground. Assuming of course that the client changes nothing as well;

4. *Continuity* – Consulting is fun, report writing, is not. 90% of all consultants feel the same way, so the documentation aspect of an engagement is usually weeks behind, or woefully inadequate. Either way, if the consultant you've assigned leaves, you had better have a *very* comprehensive way of handing over the gig to the new guy to ensure that they are not starting all over again; and
5. *Value* - No-one likes being taken advantage of, so whatever you sell had better deliver what was promised. Or better, also with some form of value-add.

What's more, selling them what they asked for is no excuse for selling them something they don't need. You are the expert, and you should help them work out what they need at the beginning and provide it accordingly. You may not have as big a sale as you'd like up front, but the trust you instil will ensure they'll only buy from you going forward.

Consulting Wrappers

If yours is a product only organisation, you will need partnerships with consulting organisations that put your product into the necessary context for the client, and perhaps even set it up and managing it for them. Too many appliances sit on IT manager's desks because they had no idea what to do with it once the salesperson left.

Patience

Selling security is an iterative process, and you must be prepared to hold-off on the big POs until the client is ready. Sell them what they need, only when they need it, and especially only IF they need it.

Doing this requires a degree of management buy-in that is all but non-existent today, especially in the American sales process, where the never-lose-a-deal-over-price attitude forces the salespeople to sell as much as possible, as soon as possible. Any organisation that sells this way can never, ever, call themselves Trusted Advisors.

Courage

The ultimate in security salesmanship is a salesperson that actually refuses to make a sale because it's not right for the customer. You can image how often this happens, and I'm sure the phrase 'naïve idealist' immediately sprang to mind (or worse).

But the whole point of being a top-notch security salesperson is NOT to sell, that's an automatic by-product of being the person organisations call to resolve their challenges. The extreme would be to offer suggestions of your competition that are better placed to help the client at that particular juncture, knowing the client will come back to you to take them the rest of the way. The 'rest' is always the vast majority of the eventual spend.

Once again, upper management needs to embrace this paradigm or no salesperson will dare. It's worth it though, and a salesperson should be every bit the Trusted Advisor that the consultants are, and eventually, the so should the company as a whole

THE PROCESS

I'm making the assumption that your organisation is able to provide complete security solutions including consultancy / product / managed services etc., either directly, or though partnerships / channels.

Phase I - Opportunity

Step 1: Sales (Hunter) brings opportunity to the consultancy department for scoping;

Step 2: Consultancy assigns appropriate resource for pre-sales SME support;

Step 3: Sales (Hunter) reconnects with client to introduce SME, who in turn confirms client has correct representation for the scoping call;

Step 4: SME and client conduct scoping call to ensure the Work Statement is accurate, appropriate, and achievable in the agreed timeframes;

Step 5: Sales (Hunter) closes deal, consultancy assigns resource;

Step 6: Sales (Hunter) introduces Sales (Grower) to client as on-going Account Manager

Phase II - Delivery

Step 1: Consultant delivers work as specified;

Step 2: Consultant and Sales (Grower) discuss project and possible next steps;

Step 3: Sales proposes to client the next steps in the security program Development;

Step 4: Cycle repeats, or ends

Phase III - On-Going Account Management

Step 1: Sales (Growers) and Consultants stay in touch with client, and each other, to provide continuity of guidance, and to work on achieving the 'Trusted Advisor' status;

Step 2: All changes in the threat landscape and compliance / regulatory space are opportunities for proposal to the client, but always in the client's own 'language'

The whole point of this sales process is to ensure that you are the preferred provider of every security service necessary to keep the client in business securely, and responsibly.

The consultancy portion is to make sure that no opportunity is lost, which is not achievable though sales alone

WHAT TO SELL, WHEN, AND WHY

The order in which you sell security services will determine how *much* you end up selling, and how close you get to achieving the ultimate in business partnerships; the Trusted Advisor.

It is the difference between a one-off sale, and a lifetime partnership, and it goes against almost every sales process I've ever seen.

Traditionally, the sales process includes two 'immutables'; sell it fast, and sell as much as you can. This is diametrically opposed to how you sell security properly; take your time to make sure you've got it right, and sell only what's appropriate at the time.

When compliance regimes like PCI, HIPAA, even GDPR are enforced, organisations naturally ask for security expertise to get them through it. They end up getting what they asked for, and not what they really needed. As a security salesperson, it's your responsibility to help them ask the right questions.

Phase I – Education

A minimum of 1, and a maximum of 3 days training and presentations on a range of subjects and audiences, geared towards 5 goals:

1. Address the questions they asked, and more importantly the one they didn't. Here is where The 6 Security Core Concepts are introduced to put what they asked for into the correct business perspective;
2. The most senior management available (preferably the CEO) is requested to make an appearance to say what equates to; "I'm here, obviously this is important to me, get it done." I estimate that this alone will save the client up to 50% of the impact to their internal resources. Management buy-in, even the *appearance* of it, is critical to success. The biggest benefit however is this is how the necessary change in culture begins;
3. Let every stakeholder in the organisation know what's next, and what their role is going to be in it. This is the baseline from which the rest of the relationship stems, and without it, the client has no idea that the security process has only just begun;
4. Introduce what else you are capable of delivering, especially the concept of Risk Assessment and Business Impact Analysis. This is a NOT a sales pitch, just an opportunity to let them know they really don't have to look anywhere else to solve their security challenges; and
5. Put faces to names, especially yours. This subject is a white paper in and of itself, but suffice to say, it's much more difficult to ignore communication and guidance from someone you've actually met, than from someone who is just a name. It's human nature. Chances are you will also be seen as an 'auditor', or at a minimum an unwanted distraction, so unless you can show that you are there to help, your task becomes unnecessarily difficult.

Phase II – Risk Assessment

Unfortunately there is roughly a 99% chance that your potential client has not performed this most fundamental of all Security Core Concepts. Without a risk assessment you have no business goals, no baseline, and no indication of data-value from which to begin the development of a sustainable and *appropriate* security program.

I will not go into detail, you can find that in these three blogs:

- The 6 Security Core Concepts
- Security Core Concept 1: Risk Assessment / Business Impact Analysis
- Security Core Concepts: Tying it All Together

…but unless the client understands the importance of this step from both you, and the Education Phase, all subsequent phases will not be as effective and security will be negatively impacted in terms of effectiveness and value.

I simply cannot stress the importance of this phase enough, as you need an indication of the following things to know what to do next:

1. The value of the data – speaks to budget and management buy-in. If the data is worth £1,000, don't spend £10,000 to protect it. The other way around makes sense though;
2. The goals of the business with regard sustainability and growth – speaks to appropriateness of solution in terms of current and future needs; and
3. *How* the organisation performs its business functions – speaks to scope, complexity, and required skill-set requirements.

Phase III – Control Gap Analysis / Health Check

Different regions call it different things, but what it means is the same thing; to what extent does your current security infrastructure meet the requirements of the business?

The risk assessment began the process of defining:

1. The full extent and type of assets – this is not just computers, this is applications, people, locations, documentation, and of course data;
2. The data-flow and storage processes – what do you do, how, and why?
3. Exactly what is required to *stay* in business

The gap analysis goes much further, and ends up with a 'laundry list' of everything that needs to change in order to meet the goals as defined.

What this does NOT do is tell the business HOW to fix everything, that comes next.

Phase IV – Remediation Guidance & Control Definition

This is where the rubber meets the road and other similar clichés. In the previous phases, you have defined exactly what they need to stay in business appropriately, where they are right now, and what the gaps are between the two.

Now it's time to help them do the following, and in this order;

1. Closely examine current business process to see if there are any immediate changes that can be made to reduce risk, and potentially, increase efficiency. OK, so that last part is not strictly security relevant, but this is supposed to be a partnership, and any value-add will pay dividends.

   What you are fighting against here is the but-we've-always-done-it-this-way mentality;

2. How can their existing infrastructure be adjusted to fill the gaps? Few clients will have the necessary in-house skill-set to design an optimal architecture, and the chances are they have been throwing technology at process challenges;

   The temptation here is to sell them product and services to fill the gaps, but that goes against everything I've written up to this point. To show your true value, and values, this step must come first;

3. Additional technology, or specific remediation services, offered in the following order:
   i. minimal capital outlay (but probably require significant in-house expertise),
   ii. modest capital outlay (more off-the-shelf / intuitive), and;
   iii. 'other' (assuming they are still appropriate to the environment in question);

4. Define the next steps. There is no use bringing them this far without taking them the rest of the way. Now that you have proved your worth, the client will generally be far more open to conversations of how to take the work performed to date are continue the development of the full security program.

   They may not want to anything at this stage, *usually* don't in fact, but if/when they do, you can be assured that will not be looking around for anyone else.

Analogy: You have a headache, do you go straight to a specialist and ask for brain-surgery? Of course not, but this is exactly what clients do if you let them. First you take an aspirin, then maybe something stronger, then you go to a General Practitioner who THEN and ONLY then refers you to the specialist.

Sell security the same way and you'll always be in line for the client's next requirement.

Don't do this and you'll lose their trust forever.

SELLING TO THE VALUE NOT THE COST

I have broken this into its own section for several reasons, but the two most important relate to 1) discounts, and 2) perceived value.

In most sales processes, especially the US ones, the concept of discounts is as ubiquitous as the sales process itself, which leads to the universally accepted idea that the services are not worth the original price.

Security is now just another commodity to be bartered, and eventually assigned to the lowest bidder.

The 'winning' provider must provide what was sold at a profit, so the end result is that the client gets *only* what they paid for, which will never come anywhere near what was needed.

Discounts are only valid in these scenarios:

1. Client loyalty – offer a discount for their loyalty, which does *not* mean multi-year deals, it means they have stuck with you no matter what;
2. They buy more of what you were originally trying to sell, or add other services / product not part of the original opportunity;
3. They provide additional benefit to your organisation; referrals, case studies, references etc.

As for the perceived value, if you are being underbid, it could be a number of factors over which you have no real control:

1. You *are* too overpriced;
2. Your competition has worked out how to deliver similar services more efficiently;
3. You have misunderstood what the client actually needs

More likely it's one of the following:

- You have gone in high, assuming you'll have to come down some;
- Your competition is new to the game as is prepared to take a loss to build their client base;
- Your competition is very good as writing statements of work that will definitely involve some kind of scope creep at the client's expense

You simply cannot play these games and maintain the sense of integrity you need to sustain the type of partnership / relationship I have referred to throughout this white paper.

Work out what your services and products cost to deliver, decide on your profit margin, and stick to your price-list.

SUMMARY

I'd like to think that this white paper speaks for itself, but there is simply too much that goes against standard and traditional practices to be widely accepted, if at all.

However, like I said previously, this is really designed to break down for buyers what *they* should be looking for in terms of security partners and services. In other words, this paper has defined how they should buy a security program that is best for their business, and how to choose a security company that best able to provide it.

But mostly, this paper is about integrity and values, and how they must be intrinsic to not only each individual in the process, but for the organisations whom they represent.

Finally, I will repeat the phrase that forms the motto of my own business;

Security is not easy, but it CAN be simple.

Selling security is no different.

ABOUT FROUD

David has almost 20 years of experience in areas of Information / Cybersecurity, including Regulatory Compliance, Secure Architecture Design, Governance Frameworks, Data Privacy & Protection, and FinTech.

As Project Lead for several Fortune / FTSE 'Enterprise Class' clients, David has performed hundreds of on-site PCI, security, and regulatory compliance assessments for organisations globally.

Blog: http://www.davidfroud.com

Linkedin: http://www.linkedin.com/in/davidfroud

ABOUT CORE CONCEPT SECURITY

Core Concept Security (CCS) is an independent cybersecurity and data protection consulting practice based in the UK, but available globally.

The guiding principle behind all CCS's services is that security, while often difficult to achieve, has always been, and will always be, simple. There are no shortcuts to security, and there is nothing to be gained by just throwing money at it hoping the problems will go away. Technology will never fix what's broken, only people and process can.

The CCS approach is also simple; It's our job to help you ask the right questions, even if we aren't the ones who can actually answer them. You're hiring us, you're hiring everyone we know.

In the end, if your security program is not appropriate to your business needs it is a waste of your time and effort. Our commitment to our customers is to never settle for less than, or try to sell you anything *more* than, what you need.