



The Art of Cybersecurity Persuasion

Introduction

Many Chief Information Security Officers (CISOs) complain about a lack of executive board support for cybersecurity. I regularly note discouraging posts on LinkedIn about the difficulty of persuading senior executives to embrace best practices and fund the necessary technology and resources to secure business assets. My personal experience, however, (and I have worked with organizations of all sizes and sectors) is quite different. I have rarely, in fact, experienced any difficulty in persuading senior executives to invest in cybersecurity, though some have been more willing to follow my advice than others.

How is it that I seem to succeed where others do not? The answer is simple. It's not because I have any magical charisma or personal powers of persuasion. It's because I collected, developed and deployed many practical techniques to help sell cybersecurity. Some of these I mentioned in my 2009 John Wiley book *Managing the Human Factor in Information Security*.¹ But others remain unpublished. This paper sets out of my portfolio of “tricks of the trade” for persuading people at all levels in an organization to support, fund and adopt best cybersecurity practices.

You can find books, articles and videos that claim to teach how to persuade people of various types to accept your demands, including customers, appointments boards, love interests or even secret agents.² You can also find papers by experienced CISOs, such as *The Art of Influencing* by Phil Venables, a former top CISO, which outlines useful business techniques for influencing people.³

This paper is a little different as it is essentially a collection of lesser-known psychological tricks, smart strategies and good ideas that I have found to work in selling and implementing cybersecurity. And it's written not just for aspiring mesmerists, but also for ordinary professionals who are designing awareness campaigns. In the words of Mark McCormack, this paper is really about “What They Don't Teach You at Havard” (or perhaps Royal Holloway University of London if you're a *Da Vinci Code* fan).⁴

1 “Managing the Human Factor in Information Security: How to win over staff and influence business managers Paperback” by David Lacey, January 2009, Wiley, ISBN-13: 978-047072199523.

2 For example, a popular book aimed seemingly at sales staff and con artists is *Covert Persuasion: Psychological Tactics and Tricks to Win the Game*, Kevin Hogan, September 2006, Wiley, ISBN-13: 9780470051412. Also, a classic book on the secrets of effective large-scale leadership is *Leadership Secrets of Attila the Hun*, Wess Roberts, February 1990, Business Plus, ISBN-13: 978-0446391061.

3 See <https://www.philvenables.com/post/the-art-of-influencing-7-steps>.

4 *The Da Vinci Code*, Dan Brown, March 2003, Vintage, ISBN-13: 978-0385504218. The cryptographer in the best-selling novel claimed to have been educated at this university.

Where to Start

Whatever and whoever you wish to change, the starting point is to define the precise nature of the change you wish to bring about and the target audience, whether it be an individual, a management team, a business unit, a geographic region or an entire enterprise. As we shall see later in this paper, designing interventions to successfully achieve a particular type of change is much more complex and sophisticated than you might first imagine. There are specific factors and considerations that determine the most effective type of intervention for the type of change you wish to bring about.

Understanding and addressing them will be the difference between spectacular success and abject failure.

Ask yourself: What exactly is the nature of the change you wish to make? Do you want to influence a CEO or executive board, sell a project or funding proposal, or transform the awareness, attitudes or behavior of a business unit or customer? These objectives might at first sight seem to be similar challenges. But each demands a different type of intervention. To change an individual person's attitude requires a very different approach from transforming the behavior of a large group of people. And as we shall see, changes in *awareness*, *attitude* and *behavior* require very different strategies and techniques.

Politics and personalities are also important considerations when it comes to persuading senior managers and directors to accept your recommendations. Many CISOs recommend adopting “business language” when addressing executive boards. Personally, I really have no idea what this means. And I have never found such an approach to be necessary or useful. It is, of course, essential to understand your organization's business strategy and principles. But I've never been asked or expected to manage an organization's business. And few business managers are likely to seek my advice on how to increase sales and profitability. Essentially, they simply want me to sort out their cybersecurity quickly, cheaply and effectively. That's the kind of conversation they prefer to hear.



Timescales, scope and sequencing are also important considerations for any desired change. Are you looking for a quick, easy improvement or a lasting transformation? And are you hoping to use the same approach and material across different levels of management or geographic regions? Using a standardized program across multiple jurisdictions is a challenge, as different cultures may have varying perceptions and decision-making processes. Things that we might expect to be universal, such as humor, style or risk perception vary significantly across enterprises, countries, cultures and communities. What works in the USA might not work as well in Europe, Middle East, Africa or Asia. And business mindsets can be very different even in neighboring countries such as Sweden and Norway.

Timing of interventions is also important. A certain degree of education and awareness may be needed prior to launching a more ambitious initiative to achieve a larger and longer-lasting change in employee behavior. And if you wish to gather hard evidence of the effectiveness of your achievements, it's useful to first measure your audience's initial knowledge and attitudes (e.g., through some form of questionnaire) before embarking on your initiatives.



Understanding Organisational Culture

Understanding the organization's culture is a vital consideration before promoting cybersecurity. By "culture" I mean the underpinning values, attitudes, behaviors and norms that define how staff perceive and translate directives into action. These factors can be similar across many organizations, but they are not universal. Values and norms will vary across countries, ethnicities, religions, age groups and individuals.

Appreciating such differences is particularly important when operating in an international environment. A recommended starting point is to read Dr. Mandeep Rai's excellent best-selling book *The Values Compass: What 101 Countries Teach us about Purpose, Life and Leadership*.⁵ Mandeep concisely sets out the most significant value associated with each of 101 different countries, whether it be pragmatism (China) or problem-solving (Cuba). Understanding the values that specific regions or cultures care about helps in promoting cybersecurity to both local and international staff.

Appreciating organizational culture is a surprisingly difficult challenge for those working within the enterprise, as staff are generally blind to many of the views and practices they have unconsciously absorbed, sometimes against their better judgment. Most employees will be indoctrinated over time to accept and adopt organizational perspectives, however unfamiliar or controversial they might seem at first. Behavior considered strange, different or even unacceptable to an outsider can appear “normal” to a long-serving insider. An outsider or a person new to the organization is generally better placed to recognize its true nature.

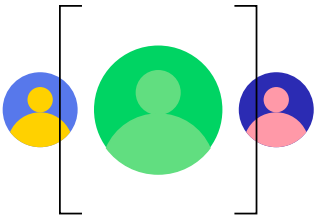
Long-embedded values and cultures can be challenged by new markets, fashions and appointments. Enterprises that take on fresh groups of staff through expansion or acquisitions can suddenly gain a fresh set of perspectives. Appreciating both old and new perspectives is important when pitching to executive boards or designing awareness campaigns. Transforming perspectives requires more than just good communication. It also demands an analysis of the factors that promote specific attitudes and behaviors. And these are not the same. Attitudes are shaped by personal experience, but behavior is influenced by perceived consequences. Identifying the underpinning motivators of people's actions requires considered thought and analysis.

Another aspect of organization culture that we must acknowledge is so-called “security culture”: the idea that some communities embrace security, yet others appear to dismiss it. The fact that some groups are good at security, whereas others are not. It's also important to recognize the spectrum of possible security regimes, ranging from healthy ones built on empowerment, trust and openness, to more sinister ones based on fear, blame and punishment. Is there a single, best means of achieving a perfect security culture? I once asked Dr. John Meakin, a seasoned CISO who has led functions in many leading Fortune 500 companies, for his views on security culture and how it changes across communities. He replied:

“I have seen two different cultural groups take the same policy, technology and processes, and one succeed in making systems more secure, while the other succeeds in making them less secure. Maybe a one-size-fits-all approach to security technology and process isn't right.”

Every organization has a unique blend of cultures and perceptions, which can vary across professions, business units and sites. Some cultures challenge new ideas; others prefer to obey leaders. Some individuals are risk-averse; others throw caution to the wind. Some front-line staff are smart in dealing with third parties; others are excessively trusting. Personal experiences, both inside and outside the organization, determine this.

For maximum effectiveness in influencing employees, we should adjust our presentation style, marketing techniques and governance methods to specific environments. I have, for example, witnessed a Chief Information Officer (CIO) present an identical speech to different international sites and receive completely different responses, ranging from wild cheers, through complete silence, to aggressive challenge. Some ideas and themes will be universally successful, but it's rare to find a single approach that works best in every site and circumstance.



Responding to Organizational Politics

Whether we like it or not, many managers have an unfortunate tendency to compete with their peers, spurred on by personal choice, organizational culture, or perhaps because Human Resources promote leaders and punish laggards. Some enterprises tolerate or encourage backstabbing and power-seeking (investment banking in the 2000s comes to mind). Others promote and reward teamwork and collaboration. But most organizations financially reward financial success, so there is always an incentive to perform better than your peers.

You might yourself be, or report to, a people-pleaser or a closet psychopath, but you should always adopt your approach to cater for all personality types. Regarding politics, you can study Machiavelli, who believed that the end always justified the means, but followers of his advice can be unpopular and short-lived.⁶ And it's important for a CISO to strive for universal popularity, because cybersecurity cuts across every part of the organization. You should recognize and take account of office politics. But under no circumstances should you take sides, because you might alienate other managers. And unforeseen events such as market changes, new senior appointments or mergers and acquisitions can suddenly undermine the underlying power structures within an organization.

⁶ Niccolò Machiavelli was a Florentine diplomat, author, philosopher and historian best known for his political treatise *The Prince* (ISBN-13: 978-1954839274). He has been called the father of modern political philosophy and political science.

⁷ *How to Win Friends and Influence People*, by Dale Carnegie, International edition, February 2017, Manjul Publishing House, ISBN-13: 978-8183227896.

CISOs should resonate with all management teams. There is no room for favorites and enemies. And popularity is not all that difficult to achieve. This is where those popular paperbacks I alluded to earlier can be useful. I would recommend that you take a leaf out of Dale Carnegie's classic book, *How to Win Friends and Influence People*.⁷ His most powerful trick is simply to treat people well and avoid unnecessary criticism. Criticism does not win friends but will create long-term enemies. Note also his suggestion that the sweetest sound to a person's ear in any language is *their name*.

Cybersecurity rarely costs or enables new business opportunities. It can happen, of course, but it's hard to predict or measure. Unsurprisingly, therefore, many executives will view cybersecurity as a waste of money, a necessary evil or perhaps a barrier to new technology adoption. At the same time, cybersecurity can be viewed as a cornerstone for enhancing corporate reputation, maximizing brand value and helping to safeguard intellectual assets. We should always promote the latter, but also anticipate and defend against the former, regularly drawing attention to the positive benefits in the minds of senior executives.

The smart CISO builds relationships with both the champions and enemies of cybersecurity. Corporate functions such as Audit, Legal and Compliance will be powerful advocates of security and should be encouraged to articulate its benefits. Business managers on a tight budget can become cybersecurity blockers, so should be helped to balance their books. Look for ways to enable them to save money, for example through standardization, consolidation or outsourcing of services.



Understanding and Influencing the Executive Board

Nothing substantial gets done without executive board consent, so this is the best place to begin your initiatives to promote cybersecurity. Boards can make things happen, even when corporate politics and rules are against you. I have seen the most hard-nosed senior executives respond to magnificent pitches that sought to bypass corporate policy and rules. I recall one chairman, for example, respond to a spellbinding pitch for much greater investment in ecommerce with the memorable words: "I don't care about the business case. I'm backing you!"

You should start by recognizing and absorbing what is termed the “tone at the top,” the ethical atmosphere created by the organization’s leadership through their decisions, actions and communications.⁸ This behavior sets the standard for the corporate culture of the organization, exemplifying how the enterprise must balance its desire to maximize profit against more principled considerations such as business integrity, regulatory compliance and fraud prevention.

Uniformity used to be a characteristic of many executive boards but that has changed as boards have become more diverse. This is a good thing as it helps to discourage “groupthink,” a phenomenon that affects many executive boards.⁹ Groupthink encourages individuals to make less-than-perfect or even quite stupid decisions in the interests of achieving consensus decisions. I have found this phenomenon even more pronounced in crisis teams, where members feel pressured to make speedy decisions to help resolve the crisis as quickly as possible. CISOs need to be alert to when groupthink is setting in on any unwelcome major decisions on cybersecurity and aim to influence individuals to ignore such influences on their own thinking.

Executives from many types of background can make up an executive board, though some form of financial experience or qualification is generally desired. Oil companies might appoint an engineer or an accountant as their CEO, which could have a major influence on board priorities. Ambitious companies aiming for rapid growth might employ a mergers and acquisitions specialist, which could shape an entirely different board perspective. Executives with different backgrounds might interpret corporate policy in different ways. Some will be risk-takers, others risk averse, often reflecting the nature of their formative line of business. Within a bank, a former derivatives trader is likely to have a different risk perspective than a former credit risk manager. Interestingly, I have found that the most distinguishing factor among senior executives is the speed with which they arrive at decisions. Former traders are exceptional at this.

You should try to get to know the individual views of as many board members as possible before making assumptions about the organization’s risk appetite and compliance priorities. These views might vary according to the relative importance of specific products and regions, and the likely impact of a major incident in an important market. How do you get access to individual board members? You simply ask. Most directors will spare the time to speak to an informed cybersecurity specialist. Start with the chief executive and work downward. It’s surprising what you can achieve, even in a few minutes of discussion. Be prepared to listen rather than dictate. Ask open questions to get the broadest reaction. And if it’s going well, don’t hold back on bringing up any reasonable demands you might have.

⁸ The term “the tone at the top” was coined by the Treadway Commission in 1987, reporting on financial fraud. It highlighted the importance of top management in setting the ethical tone for financial reporting.

⁹ “Groupthink” is a psychological phenomenon where the desire for harmony or conformity within a group leads to irrational or suboptimal decision-making.

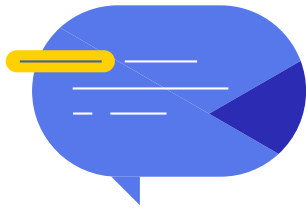


Gaining buy-in to cybersecurity programs requires more than just sound ideas and good content. When presenting to an executive board, you should always consider the style of your presentation before assembling the content. You need to get into the minds of executive directors and appreciate their personal perspective, which is likely to be very different from your own. Directors are bright, busy people. Their job requires them to deal with many fast-changing issues in a very short time. They will quickly grasp the points you make and will absorb information faster than you can explain it to them. But their patience is limited. You will annoy them if you talk down to them. And they may jump to conclusions, so you will need tactful interventions to keep them on the right track. Your presentation must be slick, compelling and to the point. It's not guaranteed they will have read any briefing papers you forwarded in advance. And your available time might well be curtailed if the meeting is running late. You should anticipate running out of time and have a prepared summary that gets your major points across before or when you are cut off.

Keep an eye on their body language. If they look uncomfortable, summarize your latest points and quickly move on. If they look confused, ask them very politely, "Are you with me so far?" And remember that first impressions count. People will judge you as soon as you walk into the room. Be confident, compelling and authoritative. The board may not be familiar with your own expertise, capabilities and achievements. They will quickly decide whether you are an expert or a charlatan.

If all else fails, it's worth having a threat or two up your sleeve. The late Professor Fred Piper, for example, once told me he was hired to advise an executive board of a leading British bank on the urgent need to upgrade their security.¹⁰ They were not impressed with his advice until he said, "Well, if you're prepared to accept the liability," at which point the entire mood of the board changed and they listened more attentively to his recommendations.

¹⁰ Fred Piper was a leading cryptographer who founded and led the cybersecurity MSc courses at Royal Holloway University of London.



Mastering the Elevator Pitch

You never know when you will be in an elevator with the CEO or perhaps walking alongside them on the way to a management meeting. It has happened to me many times. In such an event, you should always be ready with a well-thought-through set of points to make or perhaps a very short “elevator pitch” to summarize your ideas or demands.

You should also have a short summary of anything you present at important meetings, as it’s always possible that you’ll be interrupted and not get to finish your full speech. And whenever you speak to the media, it’s useful to begin with a 4- to 5-second summary of your talk, as this will provide the reporters with a ready-made headline or introductory “teaser” of your choice. And be prepared with a good holding reply to any questions you cannot answer. Never say: “I don’t know.” Say something like: “I’m getting an up-to-date briefing on that later today. Can I get back to you with the latest position?”

Always take advantage of informal opportunities to talk to board members. Sometimes you can hit the jackpot. For example, when I was recruited to lead the Information Security function at a large organization, I was invited to meet the CEO in my first week. I had only been in place for a few days but had already noticed a problem with budgets. There were many of them and some were quite sizeable, but none were under my direct control, and many were being wasted on expensive consultants who were delivering little value.

The CEO (John) welcomed me, and we had the following conversation.

John: “Welcome to the group, David. What are you going to do for us?”

Me: “Well, John, with your support, I’ll build world-class information security across your entire organization.”

John: “That’s amazing. How long will it take?”

Me: “With your support I think I could achieve 80% of that within 18 months. Is that OK?”

John: “That’s fantastic. But how much will it cost?”

Me: “With your support, not a penny more than you’re currently paying, as long as you give me control of all the relevant corporate center and business unit budgets.”

John: “You have a deal. Come and meet the group finance director.”

Within 10 minutes, I had achieved greater control of spending as well as gaining the support of two of the most important decision-makers. Simple and effortless. I had, however, also made a firm commitment to deliver on promises. My neck was on the block. But CEOs like that. They don’t want to give you more money, but they’re happy to see better results for the same cost. And they like people who take the blame as well as the credit.

You should always be ready to take advantage of such unexpected opportunities. But be careful to reserve your best proposals for the right person, at the right time and place. “Keep your powder dry,” as they used to say in the days of flintlock muskets.



Where Power Lies

As the famous novelist Alice Walker put it, “The most common way people give up their power is by thinking they don’t have any.”¹¹ This maxim most definitely applies to CISOs. Many believe they lack the authority to force business managers to address cybersecurity. But they are wrong. Real power isn’t necessarily something conferred on a person. It’s more about how other people respond to you.

And that is governed as much by your personal skills and credentials as well as your formal position. These credentials can be wide-ranging. They might include your reputation, your expertise, your communications skills, your personality, your tactics and your influential supporters, to name a few.

For ten years, I was the Shell International Principal Information Security and Business Continuity Group expert, responsible for policy and advice to all Shell Group companies. Like all Shell International advisers at that time, I could advise on but not mandate changes to Shell operating companies. Yet within a few years I managed to obtain independent BS7799 (now ISO 27001/2) accredited security certification for all Shell IT services across Europe.¹² And a few years later, we were able to implement a more rigorous and comprehensive certification scheme across around 200 sites in 130 countries.¹³

¹¹ This famous Alice Walker quote was first published in an interview titled “A Long Walk to Freedom,” which appeared in the print edition of *The Guardian* newspaper on February 25, 2001.

¹² KMPG certificate No 1, awarded under the Dutch BS7799 accredited certification scheme. BS7799 was a British Standard published by the British Standards Institution in February 1995. It was the basis of the International Standards ISO/IEC 27001 & 27002 published in 2005.

¹³ The Shell certification scheme was founded on the concept of an international “Trust Domain” to enable knowledge sharing between Shell operating companies. The scheme was based on a subset of BS7799 controls augmented by technical implementation standards for networking technologies.

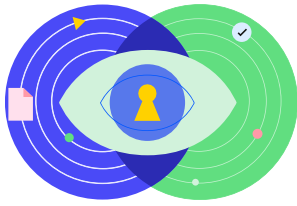
How did I achieve this? Firstly, by early adoption and aggressive promotion of a high-quality new British standard. And secondly by continuously extending the scope and detail of our guidance. And thirdly, and most importantly, by persuading the board to accept a single security rule: that to be entitled to connect to the Shell Group international network, each site must be independently certified by an approved local auditor to a set of our specified standards.

Later, for the British Royal Mail Group, I achieved the world's largest BS7799 accredited certification, covering all data centers, user areas and outsourced services. This was achieved mainly through sheer persistence. We assembled a project team that continuously harassed every local manager into complying with the controls. And we briefed all key individuals immediately before each audit on the likely questions the auditor might ask. (You should always accompany auditors throughout their interviews, both to advise and to learn.)

Simple, well-thought-through strategies, smart tactics and perseverance are the keys to success at all levels, at all scales and in all environments. When you are attempting to persuade hundreds of managers to carry out small tasks to a strict timetable, you need to ask them more than once. Persistence pays dividends. So, the most important traits to look for and encourage in your team are tenacity, determination and sheer doggedness.

One trick I have used to good effect is to carry out a simple "health check" across all business units or operating companies and then present the results to the board in the form of a league table. Such comparisons never fail to motivate business units and functions to improve their performance. And when managers claim they've done enough by achieving a respectable but not maximum score, you should encourage them to go that step further by announcing a prize presented by the CEO for units that score maximum points. Competitions and prizes are cheap, easy and highly effective devices to nudge managers to give priority to cybersecurity.

And don't be modest. A good, convincing pitch about yourself, your function or your achievements always helps convey confidence and authority in your judgements and advice, which helps persuade managers to listen more carefully to your recommendations. Power is there to be seized, through compelling arguments, cunning plans and even outrageous bluff, if required. And you will find that this approach to cybersecurity is much more interesting, satisfying and effective than simply laying down edicts and hoping that managers will read and obey them. As one of my colleagues once said: "Policies are controls for those that choose to obey."



Transforming Organizational Awareness, Attitudes and Behavior

Once you've worked out how your organization works and its values, priorities and attitudes about cybersecurity, you can identify precisely what you need to change and how you need to go about it. What's most important? Do you need to (perhaps first) educate the workforce? Do you wish to shape senior management attitudes? Or should you aim to transform the everyday behavior of frontline staff? Deciding which goals to pursue and in what order is important because the necessary interventions are different in style, content and delivery. It's particularly important to distinguish between the need for changes to employee awareness, attitude and behavior.

Raising Awareness

Awareness is the most straightforward change you can attempt. It requires little more than good educational material and an effective communications process to feed it to the right people in the right form. This can be achieved through presentations, emails, publications, webpages, newsletters, posters or any form of corporate publication. The main objective should be to create memorable messages and material. "Stickiness" is the quality to aim for in conveying lasting images and messages. In marketing, this refers to an advertising campaign's ability to resonate with the target audience and lodge in their memories. The concept was popularized by Malcolm Gladwell in his book *The Tipping Point* in 2002, though the concept is much older.¹⁴

People best remember things that are visual, vivid, colorful, three-dimensional, sense-laden, funny, positive and pleasant. Stickiness is also enhanced by messages that are unexpected and emotional and which tell stories. Images and analogies help. Motoring analogies have always been popular for security, comparing safety features (and their associated benefits) such as seatbelts, brakes and road signs, with security requirements and improvements. Pointing out positive but not obvious benefits helps, such as explaining how better brakes enable a car to go faster.

¹⁴ *The Tipping Point: How Little Things Can Make a Big Difference*, Malcolm Gladwell, January 2002, Back Bay Books, ISBN-13: 978-0316346627.

Paying attention to the mental models likely to be associated with your messages is also important. When thinking about security, many people visualize locks, chains, barriers and guards. These are negative associations, and such images should never be used in awareness campaigns. It's much better to get your audience thinking of positive images for security, such as trusted partnerships, teamwork and freedom from hazards. You can draw on local culture to help identify the most effective images in a particular environment. I have found, for example, that soccer is a popular image for promoting teamwork in African countries. And that family themes are a useful analogy for this in the Middle East. Note also that "hard," brash advertising is tolerated within the USA, but not welcome in many European countries that prefer a lighter touch.

Choice of words can also be important. My own contribution to the English language has been to popularize the word "*deperimeterization*," a term coined by one of my researchers to describe the collapse of network perimeters and the shift to "borderless" network security. Many people warned me that it was an unsuitable choice of word, especially for senior management. But I thought the opposite. And the word stuck. It even grabbed the attention of the computer press for a few years. It succeeded because it was easy to grasp and it set people thinking.

I liked it because it encapsulated both the problem and the solution spaces. When I presented the concept to an executive board, they responded, "Yes, we can see that this is a big issue and needs to be solved, but it's likely to be very difficult and complex to tackle." This was precisely the response I sought. Long words can be surprisingly sticky. For example, after more than 60 years I can still remember, pronounce and spell the word "supercalifragilisticexpialidocious."¹⁵ I can even pronounce parts of it backward. You can't get stickier than that.

You can spend a fortune on bespoke videos and roadshows, but some of the most effective interventions can be surprisingly cheap. One of the best ways of communicating information is to ask questions to make people think and encourage them to research the answers. People remember things better when they think, rather than just read or listen. Competitions are effective and affordable and can persuade staff to do things they would never usually contemplate, such as reading a security policy. The first time I tried this in a large organization, we achieved 10,000 additional hits on our security website followed by a measured reduction in incidents. And all of this from an outlay of a few hundred dollars' worth of prize vouchers.

15
"Supercalifragilisticexpialidocious"
is a song based on an imaginary
word from the 1960s musical and
feature film *Mary Poppins*...

If you're planning to mount a sustained campaign, then you might consider using professional support, but do use consultants selectively, and try to employ the right type of expert. Cybersecurity consultants are expensive and generally have the wrong skill set for this work. It's often better and cheaper to employ journalists, copywriters, art directors, psychologists or marketing experts, though, increasingly, AI may offer the cheapest, fastest and easiest solution.

And how do you get the attention of the board? I once asked a CIO how I could best get a key security message across to board members. "Simple," he said. "Just get it published in the *Financial Times* or *Wall Street Journal*." He was right. I tried it and it worked.¹⁶ Many top executives read these newspapers. And if you're keen on this idea, your communications function might just be able to help achieve it.



Changing Attitudes

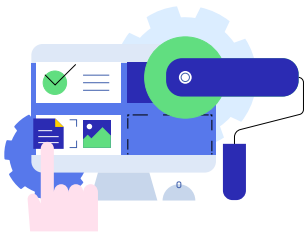
Awareness campaigns are far from sufficient for transforming an organization's actions. It's a start of course, but real change requires changes in attitudes, especially those of managers who make decisions on the actual implementation of policy and controls. Changing a person's attitude is a little harder but more powerful than simply enhancing their awareness. This is because any attitude change demands a self-discovery process in which the recipient is encouraged to suspend their disbelief and explore a different way of perceiving and thinking.

You cannot argue through a change in someone's attitude. They will probably become defensive. Attitude change requires a personal journey of some kind: a learning experience such as reading a book or magazine article, watching a video, playing a game or taking part in a creative discussion or exercise. Your audience might be skeptical or defensive at the outset, so it's important to be patient and to encourage them to suspend their disbelief as they consider the points and arguments that you are conveying.¹⁷ I have found that crisis exercises are especially effective in transforming attitudes. Exercise such as brainstorming, scenario planning or technology road-mapping are also useful as they encourage the target audience to think outside of the box and beyond their previous experience. These exercises can also generate a very useful set of outputs.

¹⁶ The article alluded to was on the importance of business continuity planning and published in the UK's *The Guardian* newspaper, a leading broadsheet.

¹⁷ Suspension of disbelief is a psychological decision to consciously set aside logic and scepticism in order to enjoy a fictional story, movie or theatrical performance.

Creating “pull” from senior management for security advice is always better of course than “pushing” information to them, much of which they will not read. One useful device I have discovered is to create a weekly or monthly *confidential* briefing paper with up-to-date intelligence on threats, incidents and vulnerabilities. I would recommend you distribute it initially only to executive board members and selected senior executives on a strict invitation-only, need-to-know basis. Very quickly, other senior managers will demand a copy and will read it to keep up with the awareness of the board.



Improving Behavior

Personally, I believe I have a very good awareness of cybersecurity, as well as a healthy, supportive attitude. But my personal *behavior* often fails to meet my own expectations. For example, I don’t change my passwords or make back-up copies of my data frequently enough. Why is this? It’s not because I’m ignorant or have a bad attitude. It’s simply because I don’t have the necessary motivators in place. Fortunately, this weakness can be corrected. But I must warn you that it’s far from easy, and, unfortunately, it’s rarely achieved in practice.

Achieving a change in behavior, especially of a large group of people, is the hardest but most satisfying change you can achieve. It’s hard because you first need to take account of the underpinning enablers and blockers of the desired behavior. And then you need to think of creative interventions to change the perceptions of your target audience. As an example, consider cigarette smoking. We all know that smoking is bad for your health. Yet many people persist. Why is this? It’s simply because the negative consequences are *long-term* and *uncertain*. Yet the pleasure gained is *immediate* and *certain*. When it comes to behavior, short-term, certain consequences will always outweigh others.

In fact, the most powerful enablers and blockers of any desired behaviors are consequences of the behavior that are perceived to be *personal*, *immediate* and *certain*. We need to identify such consequences, and wherever possible adjust them to promote the desired behavior. You can draw on both rewards and punishments for this. Rewards are more welcome and longer lasting. But they are also more expensive and harder to justify. We can, for example, readily discipline our staff, but we are rarely empowered to dish out rewards.

I have used these techniques successfully to improve staff behavior in very specific areas. I can vouch that they are surprisingly hard to apply, demanding a good deal of original thinking. But they do work.



Building a Business Case for Cybersecurity

There is, of course, more to implementing cybersecurity than simply persuading the board and the employees to accept and support your ideas. You also need money and resources, which in larger organizations requires both a budget and a business case.

In a small company, you might just need the approval of the board or CEO, but in a larger enterprise there will be many competing demands for funding. And this will necessitate the use of an agreed set of criteria for comparison of bids for money, as well as a standardized process to enable a fair assessment. In such a world, our brilliant ideas, original pitches and compelling arguments might count for little. The comparison process determines the outcome. And “bean counters” control it.¹⁸ Exceptions are rarely tolerated by the bean counters. So, if you cannot beat them, you must join them.

How do you join them? Firstly, by becoming their friends. Visit them. Take them for coffee or lunch. Tell them that you want to better understand precisely what they’re looking for so that you can present your business case in the best format for them to process. And ask if they can help you by reviewing your drafts. Questions about the construction of proposals are always well received. They will naturally want to help you because it will make their own work easier. And you might have gained a powerful supporter.

Investment appraisal functions will give you valuable insights into how to best present a successful business case. In one company, for example, they told me they were suspicious of proposals that claimed to meet multiple evaluation criteria. They also questioned proposals that appeared to be a repeat of a successful bid from an earlier year. This advice prompted me to adjust our proposals to focus primarily on a single specific investment criterion, and to always provide an explanation of how the product requested fitted into a more complete architecture of similar technologies as part of a broader “defense in depth” strategy.

¹⁸ “Bean counters” is an informal term to describe accountants who focus exclusively on numerical data and strict adherence to financial rules and budgets, often at the expense of other important issues such as staff morale and innovation.

Enterprises primarily exist to make money or deliver an important product or service, so it's not surprising to find investment criteria that focus on sales increases and cost reductions, measured of course in financial terms such as return-on-investment, payback period and net present value. But there are always other necessary non-profitable expenditures, such as maintenance, service improvements, regulatory compliance, innovation or perhaps to support the organization's business strategy. You should also draw on these to leverage your bids.

It might be refreshing and welcoming to tell the board that cybersecurity will increase business sales and reduce overall costs. But it will be difficult to present real, hard evidence to support such claims. Investment appraisal functions abhor unsubstantiated promises, wishful thinking and leaps of faith. They want concrete evidence. And if you promise to reduce future spending, they might even expect you to have approved a reduction with the relevant budget holders. So be careful with your wishful claims.

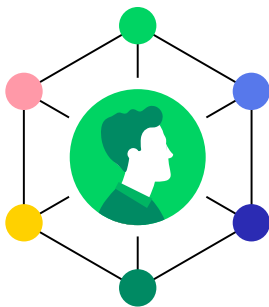
A good business case emphasizes the reason for the funding, why it's needed and why now. Justification might be to mitigate an unacceptable risk, respond to a major incident, enable an essential product feature, reduce operational costs or meet mandatory compliance requirements. Some benefits might be tangible and measurable; others less certain and difficult to quantify. Tangible, measurable benefits are the most compelling evidence. But you should also quantify intangible benefits as best you can. The best strategy for cybersecurity investment is to focus on compliance, because approval is almost certain (even in times of austerity), the budgets are ongoing and they generally increase each year with new or extended laws and regulations. A well-publicized incident will also, of course, do wonders for cybersecurity budgets.

No business case should be submitted without options, no matter how undesirable they might seem. Options should include both cheaper and more expensive alternatives. And you must always include the implications of the "do nothing" option, which sets out the underpinning justification for change.

Also, if you do not include a "do nothing" option, there is a risk that the organization might accept your argument but postpone its implementation.

If your organization likes a compromise (I encountered this for example with the British Diplomatic Service), then you should present at least three options, with your preferred solution as the middle option. On the other hand, if your management is set on ruthlessly minimizing all expenditure, then make sure your preferred solution is the lowest cost option.

In the example of Managed File Transfer (MFT), a business case would include, of course, a more secure way to transfer files. Beyond that, benefits could be: better compliance and auditability, improved visibility and automation. Tailor the business case to your organization, and you have a better chance at getting board buy-in.



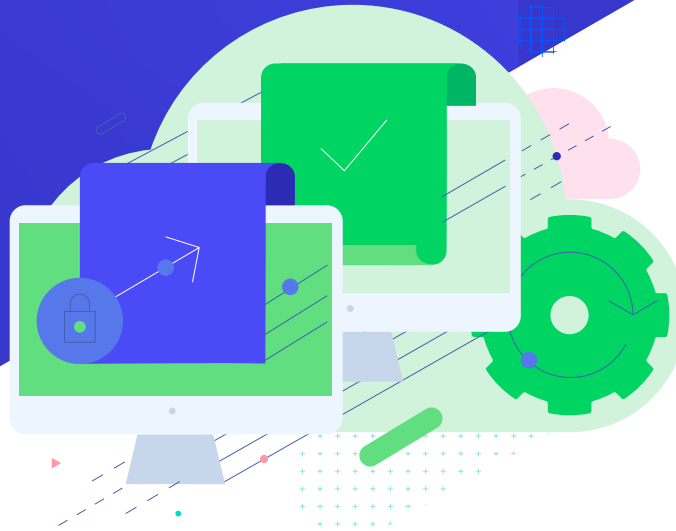
Unleashing the Human Factor in AI Governance

Governance is the essential control structure that enables organizations to verify that its operations and projects are carried out in line with business objectives and corporate policies. IT Governance has been practiced religiously for many years, initially by large organizations but increasingly by smaller ones.¹⁹ It is a necessary overhead, not only because regulatory compliance demands it, but also because major IT projects and services have a universal tendency to overrun budgets and timescales quite considerably. Badly implemented however, IT governance can become an “albatross” around the organization’s neck, an onerous overhead and bureaucratic blocker, characterized by lengthy compliance demands, stringent reporting requirements and bureaucratic approval processes.

IT governance frameworks have become increasingly detailed and complex. They are often achieved by combining several specialized industry frameworks, such as those concerned with risk management (e.g., ISO 31000), cybersecurity (e.g., NIST CSF or ISO/IEC 27001), systems development (e.g., Agile), IT service management (e.g., ITIL), IT architecture (e.g., TOGAF), as well as those specifically addressing IT governance (e.g., ISO/IEC 38500). Each one of these frameworks is a challenge for any IT professional or business manager to comprehend. Collectively, they can become an impenetrable manifesto. More worryingly, however, is the fact that IT governance has singularly failed to get to grips with the progressive growth in “shadow” (end user) computing.²⁰

¹⁹ I say “religiously” because it is performed with extreme regularity, discipline and attention to detail, and the outcome is very much an act of faith.

²⁰ “Shadow” (or end-user) computing refers to the widespread practice of staff or other end users using unapproved software, cloud services or personal devices to perform work without the oversight of a professional IT function.



Controlling shadow computing is a long-standing problem. It began with the introduction of the PC in the late 1980s, which enabled users with no IT training or experience to create business-critical spreadsheets, many with errors, circular references and undocumented changes. This practice went largely unnoticed by IT management, until discovered by eagle-eyed auditors. A second wave of shadow computing began with the introduction of commercial cloud services, which enabled business managers to purchase application systems without any reference to their IT department. We are now experiencing a third, bigger and unstoppable wave of shadow computing created by the availability of AI models that offer instant gains in personal productivity and rapid application development. No organization wishes to halt this bandwagon. But few (if any) have any effective means of controlling it.

In addition to these issues, AI injects a further set of risks and challenges, most of which are outside the knowledge and experience of everyone in both IT and business functions. AI governance might build on existing IT governance know-how and processes, but it also needs to correct its failings, as well as incorporate brand-new controls to address the many issues introduced by AI systems, such as verifying transparency, controlling bias and hallucinations, managing liabilities and mitigating new security risks and data exposures.

Governments, regulators and standards bodies have already stepped in to verify that organizations address these issues. Recent edicts, standards and frameworks published by the OECD, European Union, NIST and IEEE provide a fresh alphabet soup of mandatory demands and voluntary guidance for organizations.²¹ Further rules and standards will also be required to address the accountability issues raised by autonomous actions carried out by AI agents.

²¹ The European Union AI Act (Regulation 2024/1689) entered into force in August 2024 with fines of up to 7% of annual worldwide turnover. The International Standard ISO/IEC 42001:2023, US NIST AI Risk Management Framework 1.0 provides further guidance on expectations for organizational compliance. The IEEE has also published technical standards for AI ethics covering transparency, accountability and algorithmic bias at the design level.

These frameworks will shape the necessary policies and rules for safe, secure, compliant and risk-managed development and use of AI systems. Large language models will also be drawn on to help navigate the alphabet soup, by combining and summarizing the advice and tailoring the guidance for local circumstances. But formal guidance, in the form of policies, methodologies and standards will not solve the challenges presented by the explosion in shadow AI computing. For far too long, unsupervised end-user computing has been the “elephant in the room,” largely unnoticed, ignored or unaddressed because of both the difficulty in controlling it and the general fear of discouraging innovation and upsetting business functions.

The answer to effective AI governance will not lie in committees, policies and standards. Issuing lengthy policies and rules will have minimal impact. The real solution lies in strict monitoring of the use of shadow AI computing, supported by “sticky” awareness programs, coupled with smart attitude and behavior change initiatives. In particular, we need creative ideas to identify and promote the perceived consequences of user actions that encourage the desired user behaviors, as well as the removal of those that encourage undesirable behavior, especially the ones that are personal, immediate and certain, which are the most powerful motivators for people of all ranks and cultures.

And, of course, don’t overlook the potential for using better software systems to enforce good cybersecurity behavior and discourage undesirable practices. Smart organizations aim to avoid damaging human errors or oversights by, for example, exploiting technologies that enable centralized visibility, workflow automation and auditable operational records. Visibility and control are the keys to effective cybersecurity and IT governance.

In Conclusion

I hope that I will have convinced you that there is more to persuading business stakeholders to support cybersecurity than you might have previously imagined. Lasting cybersecurity comes from aligning people, processes and technology with good governance. Transforming an enterprise's security from top to bottom is most certainly possible, achievable and affordable. But it demands a sound understanding of the types of interventions that are the most effective in shaping the perception of people at all levels in the organization.

With the explosion in shadow computing, we need to consider moving the primary focus of IT and AI governance from the corporate center to the shop floor, and to deploy the tools and techniques that have the greatest potential to transform end-user behavior.

This paper can help you to persuade your management to support your proposals, to adapt your program to organizational culture, to improve cybersecurity awareness, attitudes and behavior, to frame successful business cases and to achieve better governance of AI developments.

David Lacey FCIS FBCS CITP
12th July 2026



Learn more about managing secure file workflows with Progress Automate MFT

About Progress Software

Progress Software (Nasdaq: PRGS) empowers organizations to achieve transformational success in the face of disruptive change. Our software enables our customers to develop, deploy and manage responsible AI-powered applications and personalized digital experiences with agility and ease. Businesses of all sizes get a trusted provider in Progress, with the products, expertise and vision they need to turn AI disruption into a competitive advantage. Millions of developers and technologists at hundreds of thousands of organizations depend on Progress every day. Learn more at www.progress.com

© 2026 Progress Software Corporation and/or its subsidiaries or affiliates.
All rights reserved. Rev 2026/08 | PROJECTID-4590

Worldwide Headquarters

Progress Software Corporation
15 Wayside Rd, Suite 400, Burlington, MA 01803, USA
Tel: +1-800-477-6473



facebook.com/progresssw



x.com/progresssw



youtube.com/progresssw



linkedin.com/company/progress-software



[progress_sw_](https://instagram.com/progress_sw_)