SEQUOIA CONSULTING

Obsessed With the Bottom Line

A Better Way

Why cybersecurity is failing businesses, and how to achieve better outcomes while improving the bottom line.

A simple non-technical guide for executives who care more about results than technology.

“There comes a point where we need to stop just pulling people out of the river.

We need to go upstream and find out why they’re falling in.”

-Desmond Tutu

Foreword

Thank you for picking up this booklet.

While it says cybersecurity on the cover, I want to assure you that this booklet is probably very different to what you are expecting when reading those words.

Despite the impression created by the cybersecurity industry, that it's all technical and complicated and hard to understand, security, the actual outcome of security is something very different.

That industry focuses on managing problems that are actually symptoms. Because the vulnerabilities that put an organisation at risk actually result from quality issues.

And that means our security issues can actually lead us to find areas of potential improvement to our businesses. Not just in terms of security, but throughout the organisation, in every function.

Because of that, by the time you've read this booklet, you'll not only have a better understanding about how to achieve security outcomes than most "cybersecurity" practitioners, but you'll be on your way to making your organisation more profitable, efficient, and more agile.

It'll be more secure too, but that'll merely be a byproduct of improving quality throughout.

Table of Contents

Foreword 3
About This Booklet 5
It's Time to Wake Up 6
That's Not Security 9
How Bad Is It? 13
How Did We Get Here? 19
Six Easy Pieces 22
- **1 – Security Isn't Security's Job** 23
- **2 – Risk Management Isn't Great** 26
- **3 – It's About Quality** 33
- **4 – It's Not an IT Thing** 37
- **5 – Strategic Use of Tools** 41
- **6 – The Missed Business Value of Security** 47

Beware the Myths 51
- **Certified Secure** 52
- **Who's Feeding the Mice?** 55
- **The Cybersecurity Skills Gap** 58

Commercialising Security 61
- **A Better Garage** 62
- **Branding Security** 66

Parting Words 68
About Sequoia Consulting 69

About This Booklet

In May of 2024, Mastercard invited me to the Cannes Film Festival to speak to their EEMEA Advisory Board (composed of senior executives and the chairmen/women of a dozen banks).

My presentation was not what you'd expect from a talk on cybersecurity: It was critical of the security industry and there was little mention of technology.

Instead, it focused on achieving an *outcome*. The outcome of having a more resilient organisation through an effective structure and maturity of process, not by compensating for the lack thereof with technology.

Particularly surprising to them was how approaching security in this way helps us find inefficiencies well beyond security that, when addressed, can drive significant improvements to the bottom line.

At the end, they unanimously communicated that this presentation made more sense to them than anything they'd ever heard about security previously.

This booklet aims to provide the core contents of that presentation to a broader audience.

An audience that needs to hear it.

I hope you find it insightful.

It's Time to Wake Up

What if I told you that most of the problems the field of "cybersecurity" deals with are preventable?

Not the breaches and incidents, but the problems that made them possible in the first place.

Wouldn't it be better to not be susceptible to these events rather than constantly work to fend them off?

What if I told you that the fundamental reasons organisations are susceptible to these breaches and incidents have more to do with poor process and quality rather than technology?

What if I told you the approach used by the cybersecurity industry, which has become enormous by doing mostly security operations as a cost centre, is actually uniquely bad at achieving a sustainable outcome of security?

By this I mean putting your organisation in a more fundamentally mature and robust state so that it doesn't *need* as much additional protection in the form of costly "cybersecurity".

What if I told you that its focus on fighting fires may actually be making things worse by taking attention and resource away from their real causes?

But don't just take my word for it. Here's a quote from one of the most progressive CISOs I know,

Drew Simonis, CISO @ HP Enterprise & Juniper Networks:

"I've long argued that the biggest barrier to security is the security team. We can't stand to solve a problem, preferring lots of ongoing operations instead. In brief, we are a massive symptom management function […] with a huge conflict of interest... how do you grow your empire if you are eliminating root causes as we both agree we need to?"

If that sounds worrying to you, it should be.

In this booklet I'll explain just what Drew means here and what you, as an executive, should know and demand when it comes to security.

I bet you understand perfectly well how a Sales, Marketing, Legal, HR, or Finance department works, in some detail too. You understand their needed outcomes and how they achieve them.

But do you have the same grasp of how your Information Security function works? Do you insist on the same depth of understanding, and give it the same level of accountability as your other departments? Most executives don't.

I wrote this booklet to help those who care more about outcomes than the technology that's supposed to get us there: executives who want what's best for their bottom lines, their businesses, and their customers.

This booklet calls out problems CEOs and CFOs are not being told about and how to address them with effective leadership, leading not just to better security but also to cost efficiencies and unexpected additional business benefits.

It is not kind to the security industry and calls out its bad practices. As such it will likely upset quite a few security practitioners, and that's fine.

I trust the best CISOs, like Drew above, to recognise these issues and be open to learning and changing in order to better serve their respective businesses.

Those who would get offended or defensive being confronted with these issues will never be my customers, but that might just be an indication that you should be.

That's Not Security

Imagine being on holiday and checking into your hotel. As you get to your floor, you notice there are rat traps along the hallway.

How does that make you feel? What does that make you think?

Now imagine getting to your room and finding a few more rat traps in there as well.

Things just got worse, didn't they?

Personally, my immediate thoughts are that this is not a good hotel, that there must be issues with hygiene attracting rats, and who knows what kind of issues are behind such bad hygiene in the first place.

It certainly doesn't make me feel comfortable.

The previous hotel I went to didn't have any rat traps and I didn't have these thoughts. It felt better.

Now, you could argue that the current hotel is better because they have rat traps and the last one didn't, but my intuition tells me otherwise.

I mean, is having no traps better? It depends.

In one hotel, they might be unnecessary because they have good hygiene and therefore no rats. But in the hotel with bad hygiene the place might get overrun if the traps weren't there.

Regardless, good hygiene leading to us not needing the traps in the first place is probably the better route.

Plus, having traps doesn't stop rats from coming. It just means that we might catch some of them once they're here. To me, that isn't anywhere near as comforting as not having the rats in the first place.

I also don't fancy finding dead rats in the traps either or wonder where they might be if the traps are empty.

And that, in many ways, is what the modern-day cybersecurity industry is like. Rat traps, highly sophisticated (and increasingly expensive) rat traps.

But the field of cybersecurity almost completely ignores why we have the rats in the first place.

I once searched for a picture of a mouse to use as part of an analogy I was giving at a speaking engagement (I'll cover it later). I wound up on the website of American pest-control firm Terminix, where they had a simple 7-step strategy for dealing with mice.

Traps were among the last things to do. Tidying, making sure there were no gaps for them to enter, thinking about where you stored things, these all came first.

I used to work at the largest IT VAR (Value Added Reseller) in the world where I routinely received

"security strategies" from organisations asking us if we could fulfil them.

These were usually shopping lists of tools (our traps), with no thought about the underlying issues causing them to need the traps, how they came to have those issues, and how they were going to get away from them. Their only "strategy" was to keep laying down more traps.

Terminix's 7-step guide for getting rid of mice was a better cybersecurity strategy than what I've seen in most organisations today.

Imagine your business has no sales leads and you ask your Chief Marketing Officer what their strategy is.

They reply with a list of tools and platforms they want to buy. No mention of the message or how it would tie into your business, products, services, or customers, and no mention as to why whatever the current approach is hasn't worked.

You'd fire them, wouldn't you?

A few years ago, I advised cyberinsurance companies on how to assess the likelihood of a prospective client getting breached. As you may know, the insurance industry jumped into the "cyber" market and immediately got hammered with claims.

Part of the problem was that they were giving organisations good scores for having a large number of security technologies. I'll never forget the look of realisation on their faces when I told them that a lot

of compensating security controls, like our rat traps, might be an indicator of significant underlying problems.

Anecdotally at least, it turns out that looking at the maturity of business and IT processes is a better indicator as to whether an organisation will get breached than the amount of extra "security" they've layered on to compensate for a lack thereof.

I've worked in organisations that had virtually no security budget where all we could do was improve the quality of our processes as to have fewer issues.

We'd be jealous of peer organisations with budget to build big security teams and buy all kinds of cool tech to detect and respond to threats and incidents.

But in every case where, later on, one of the organisations was breached, it was always the one that went headfirst on the tech and "doing cyber" that got caught out. Those who focused instead on maturing processes fared better.

In summary, buying security technologies is not the same as achieving a state of security. We need to start focusing on the outcome of security, not just rolling out mitigating technologies.

Or as I like to say, "Do less cybersecurity, do more business securely".

How Bad Is It?

Before we really get started, I think it's important to understand the scale of the problem.

And no, while many cybersecurity vendors are trying to terrify you with the ever-increasing number and sophistication of threats out there, that is not the real problem we have. The problem we have is within.

In April 2024 I was invited to a roundtable lunch dinner with a UK Member of Parliament and about 20 other security practitioners.

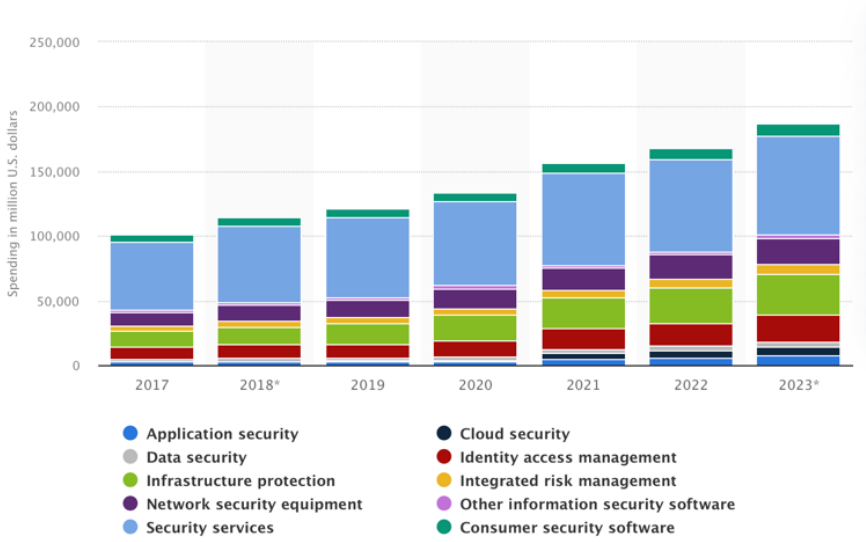
The purpose of this meeting was to help shape the UK's national cybersecurity strategy. The conversation focused mostly on how to get people to "do more cybersecurity", or rather "spend more money on cybersecurity".

I found it very frustrating. What disturbed me most was discussion of having the government essentially force people to spend money on today's cybersecurity technologies.

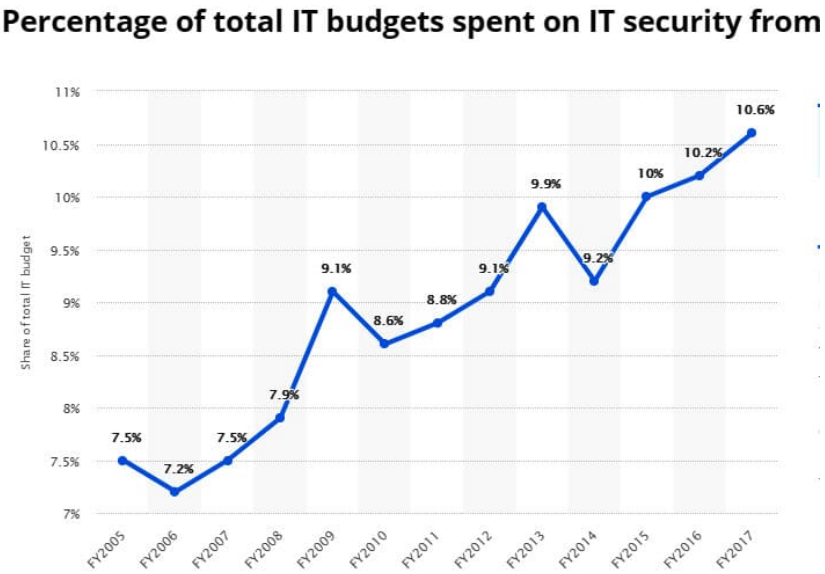
The reason this irks me so much is that, for reasons you'll understand by the end of this booklet, the current approach simply doesn't work. At least not at a macro level which is where policy should operate.

Let's look at what this room was ignoring.

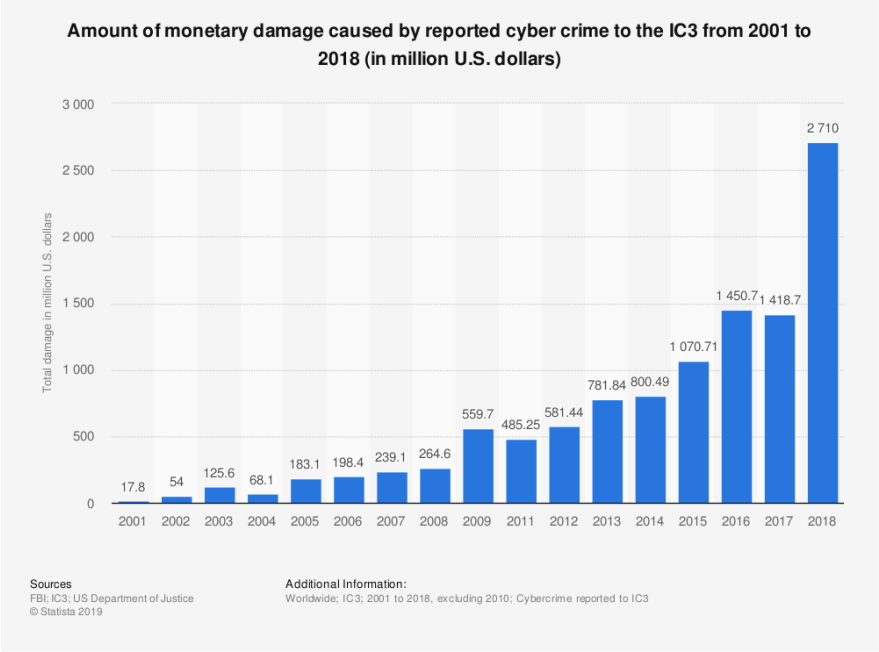
Here is one of many graphs on Google Images showing the amount of money that organisations have been spending on cybersecurity:



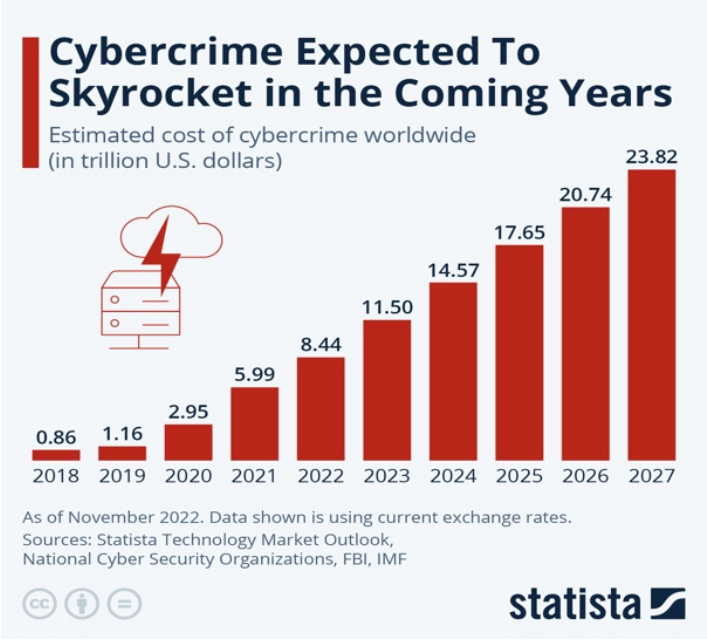
That's absolute spend. Now here is a graph of how cybersecurity costs are making up an increasingly high percentage of IT (and organisational) spend:



And here's the outcome of all that spend (lower is obviously better):



And the forecast for the next few years:



If your child had cancer and every time you went in for a treatment the cancer got worse, would you keep going?

How long would you accept the hospital telling you it will be fine if you just do more of it before you realised something was wrong and started challenging?

Now imagine if the government *forced* you to keep going. Personally, I would be mad as hell.

But I digress. The point is that things are bad, and they're getting worse in a hurry, despite us spending evermore on the problem.

Why? Well, we'll get into it but it's essentially because we're *not* spending money on the problem; we're spending money on the symptoms.

We're not addressing how we came to have the vulnerabilities getting us breached in the first place. We are instead focusing almost exclusively on managing them and dealing with the situations caused by us having them.

Consider that according to some statistics (and my own experience) more than 99% of breaches involve the exploitation of vulnerabilities that were publicly known and readily avoidable.

The security industry is very loud about selling us solutions to mitigate the risks caused by these vulnerabilities, but eerily quiet about addressing why we have them.

I once compared it to the payday loan industry in a LinkedIn post. It went something like this:

You are chronically short of money.

Solution: The payday loan.

It will get you through the weekend. Result.

But longer term, it's going to cost you, and it's not going to solve the underlying problem that you have bad financial discipline (or low IT and business process quality leading to lots of vulnerabilities that now need mitigating).

Worse still, if you keep relying on it rather than fixing the underlying problem, that problem is only going to get worse (you're even incurring costs that leave you with less resource to fix it), and things are eventually going to end up very badly indeed.

Which would you recommend to a friend? A budgeting class, getting a better paying job, or a payday loan?

Ethically, I believe we should be doing everything in our power to help the customer before issuing them such a loan. Instead, our industry flogs them like used car salesmen.

There's nothing stopping us from expanding our services to include, say, financial planning (or good security strategy and addressing root causes) for example. But the margins might not be quite as high...

Now I'm not saying cybersecurity professionals are deliberately making the problem worse. Many are very good people.

I'm also not saying security technologies are useless because they can have huge value if used strategically, as we'll see later.

But I can say that many cybersecurity vendors are very hawkish about profits due to the industry culture of VCs and big IPOs.

Fixing a customer's problem doesn't lead to a lot of ongoing revenue when you are in the business of selling symptom management solutions.

Also, despite having good intentions, many practitioners can get quite defensive when approaches they are not familiar with (or proficient in) are presented. Especially when they take away the problem that gives them their livelihood.

But first, let's take a little detour to see how we got here.

How Did We Get Here?

The late great Charlie Munger, Warren Buffet's right-hand man, had a saying about predicting how well companies (investments) would perform:

"Show me the incentive and I'll show you the outcome."

With that in mind, please allow me to tell you a little story.

I love coffee. I have a rather fancy coffee machine in my apartment and just downstairs across the street is a boutique coffee shop that makes extraordinary coffee.

So, what do I do when I fancy a coffee?

I go downstairs, and once I get to the coffee shop, I keep on walking… to the multi-storey car park where I keep my cars. I then blast through 20 miles of country roads to a little village called Alderley Edge.

Once there, I park my car, sit down, and have a decidedly average coffee from one of the chains there.

Why?

Because as much as I like coffee, I like driving a lot more. I'm a huge petrolhead. (Expect more car-themed analogies in this booklet.) My getting coffee is usually just an excuse to go for a drive.

Now imagine if you were paying me to get you coffee.

Eventually you'd start having questions as to why it takes two hours (that you're paying for) for me to get you a lukewarm lacklustre coffee.

(I feel this hasn't happened yet in security-land due to a lack of understanding of how it works by most executives. This drives a lack of accountability that can be real problem!)

Of course, as your coffee man, I'll be the first one to offer you some solutions.

Use the coffee machine right here in the kitchen? Walk down to the boutique coffee shop downstairs?

We could do either of those things, but as the expert I have a much better answer for you:

Buy me a faster Porsche.

Now, ask yourself why most people in cybersecurity chose to get into the field?

Was it a passion for solving business problems? Or perhaps because they really enjoy optimising bottom line outcomes?

Or was it because they loved geeking out on technology, and "cyber" in particular?

Bingo.

I invite you to spend an hour at a cybersecurity conference and challenge you not to be shocked at the contrast between the sheer level of technology hype and the absolute lack of consideration of business and financial realities or outcomes.

Heck, some look more like comic conventions than business ones.

This technology bias is a huge problem, because the root causes of issues beyond technology are ignored, and the preferred solutions are almost always "cyber" ones, despite them rarely being the optimum ones for the business or its bottom line.

If security practitioners did look at the situation more holistically and saw that the issues they are firefighting are caused by things elsewhere, by things often fundamentally not technological, would they have the skills or inclination to address them? I don't think many would.

And so, without the vision, skillset and inclination to address the underlying business problems, most security practitioners tend to stick to addressing the technical symptoms with evermore complex technology, because that's what technologists love.

I know this, because I used to be one of them.

Six Easy Pieces

Inspired by Richard Feynman's classic introduction to quantum physics, "Six Easy Pieces", I want to present you with six easy to understand concepts that will allow you to better grasp how security outcomes are achieved and enable you to discern between industry hype and the kinds of approaches that really drive results.

The good news is that it's a lot simpler than quantum physics. In fact, you'll likely be startled by just how obvious and intuitive most of these are once you hear them.

I've presented these concepts to Fortune 500 companies, national governments, and at countless security conferences. All have commented finding them disruptive and helpful.

More than anything, the feedback I keep getting from audiences, especially non-technical and executive audiences, is that they just make sense.

These concepts work together, as such there is a little bit of repetition, but I think that also works to drive the core principles home.

I invite you to read them again once you've finished. You'll likely find that even more things start clicking into place which will make retention easier still.

1 – Security Isn't Security's Job

In many ways, securing an organisation is like keeping a ship afloat.

A ship lives in water which, much like the "cyber threats" out there, is constantly looking to get in through any crack that it can find.

It's inevitable for some of this water to find its way in as no ship can be made perfectly waterproof - there are weak spots like seals, joints, sometimes a door on deck is left open as rain hits, etc.

The same is true of your organisation. There will always be some gaps, mistakes, and so forth that could allow a threat to edge its way in.

But that's ok.

Ships have bilge pumps to take care of this water ingress so that the ship stays afloat.

Those bilge pumps are very similar to your typical Security function. They take care of that small amount of inevitable ingress so that you can keep going.

But if you have two-inch gaps in your hull, no seals on your propeller shafts, or the doors on deck are left open during a storm allowing thousands of gallons of water to flood in every minute, then there isn't a bilge pump in the world that can handle that.

That's also ok though, because it's not actually the bilge pump's job to keep the ship afloat.

It's the ship's job.

Every part and process of/on a ship is built with the fact that it's going to have to live in the water in mind. The bilge pump is just a small part of that, there only to handle what water the design of the rest of the ship hasn't kept out.

It's the only way. I could take a 20-storey building, fill every room with bilge pumps, and it will still sink extraordinarily quickly if I drop it into the ocean.

It is exactly the same for organisations when it comes to security. You cannot secure an organisation with only cybersecurity solutions. No matter how hard you try. You must design being secure into the business.

The security industry has led us down a path of constantly ramping up our bilge pumps, rather than thinking about how our ship (our processes, our operations, and our infrastructure) must be structured to deal with the fact that they will live in a sea of threats.

This is one of the core issues facing security today; rather than making systems and business processes themselves more inherently resilient, we are ramping up how much risk management we are doing to try and keep up with the ever-increasing problems caused by that lack of resilience.

It's not working. Not only can we not keep up (as seen in the trend graphs earlier) but costs are also increasing exponentially and, might I add, unsustainably.

Security should help us define how to build the boat so that we spend as little time needing to pump out water in the first place, not forever run and implement increasingly larger pumps to make up for a design that doesn't consider its operating environment.

This takes time, consideration, and a holistic approach. There is no quick fix to be achieved by plugging in some new technology.

But it is ultimately a lot cheaper and more effective in creating a secure organisation and, as we'll see, it might just make a better performing one too.

2 – Risk Management Isn't Great

Most cybersecurity practitioners will likely tell you that security is all about "risk management".

While reducing risk is obviously a good thing, I believe the industry's version of risk-management is far from ideal. In fact, it's very different to how mature industries do it.

It's mostly focused on mitigating technical risks found in your organisation, not actually addressing *why* you have them and preventing them in the future. It's about mitigating risks that have been created, not necessarily driving down how many risks we create.

The thought process doesn't go past the technology at hand. The practices, approaches, and structures needed to drive real change are fundamentally lacking.

Time for another analogy:

Imagine our company builds passenger planes.

At some point we're made aware that the bolts that secure the wings to the bodies slacken during flight, which will eventually result in a wing sheering off.

Needless to say, this would provide a poor passenger experience, not to mention be extraordinarily bad for business. So, what can we do?

How about we build workshops in every airport in the world and staff them with engineers and specialist equipment to continuously inspect and tighten the bolts after every flight to minimise the risk of the wing coming off on the next one?

It would slow things down a bit and there would be an operating cost that would scale with the cost of the fleet, the risk would never be zero, and even if you maintain the probability of a disaster *per flight* as low as possible, the risk of a disaster happening in a given year *will* increase as the number of flights increases.

But hey, we are technically managing the risk!

The first time I ran this analogy past a colleague (who does not work in security), I'd barely gotten to "build workshops in every airport" when he immediately interrupted me with "No you wouldn't, that's *stupid!*"

Exactly.

What an aircraft manufacturer would likely to do is work closely with all relevant parts of the business to assess why the fasteners were backing out and have the design changed so that this wasn't an issue anymore.

They'd update the production line, retrofit the planes already in the field with this new component, and the issue would be solved, for good.

There would be no ongoing cost, or risk, and what they learned about the issue would help them prevent introducing similar risks in the future.

This approach just makes a lot more sense, from a risk reduction standpoint, a risk reduction *over time* (reduced risk introduction) standpoint, and a business operational cost standpoint.

And yet it's not what we tend to do in security. Most practitioners don't think that way. There are endless best practices for fighting fires, but not for assessing their root causes, why the risks are there, how to model the financial benefits of addressing them, what organisational structures should be in place to make that happen, and so forth.

Plus, tech is king. Security practitioners are familiar with it, and comfortable with it.

They are far less so when it comes to solving people and business problems, influencing, cost modelling, working across departments, taking initiative, and so on.

As a result, we often end up with a focus on what can be "fixed" with technology, cyber technology specifically.

But this "fixing" is usually more akin to mitigation, and rarely addresses causality. It's therefore unable to keep the problem from reoccurring and scaling, which means more tools, more bodies, and more work. It all adds up to higher costs for the business while delivering increasingly poor outcomes.

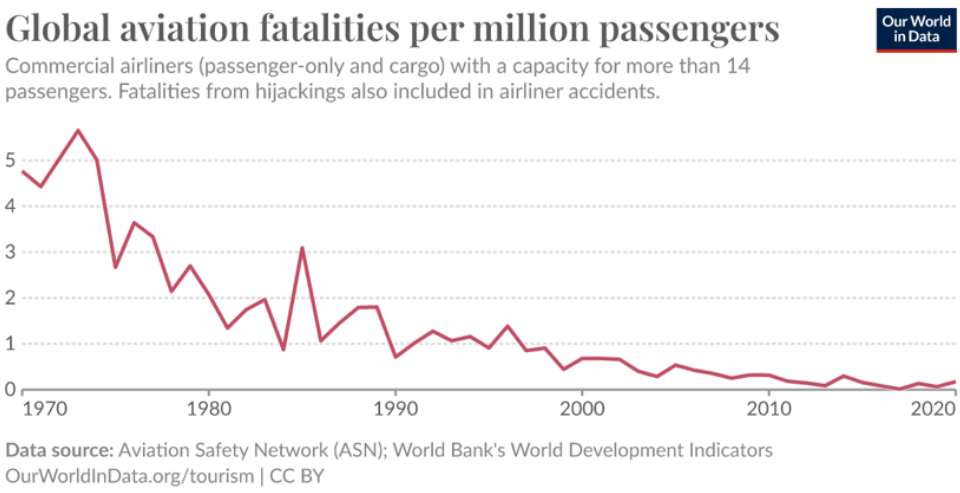
I used to be guilty of these very things, and today I feel genuine remorse about the costs I incurred to businesses at the start of my career.

It was how I was taught security was done, without ever thinking about the whole. Businesses chased me and paid me handsomely to do it too, even though they had no understanding of what tangible value it brought.

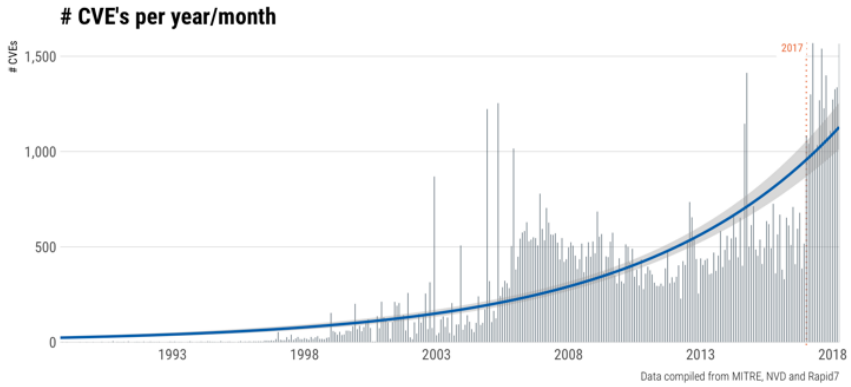
Very little, as it turned out. They'd simply been convinced by the industry that they had to.

But it's just not an effective or sustainable way of achieving a good outcome.

It's why virtually every mature industry (aviation, shipping, oil and gas, manufacturing, healthcare, etc.) has incident or defect over time rates that look like this:



While the number security vulnerabilities (and associated breaches) being discovered over time looks more like this:



And that's before multiplying them by the number of affected systems!

Mature industries focus first and foremost on root causes and maturing processes, thereby reducing the occurrence and recurrence of issues, so they don't need to fight them afterwards.

They do this until the benefit of addressing the root cause of a specific issue is no longer worth the cost of its remediation.

That's to say they only use operational risk mitigation for problems where it is too expensive to address the root cause, and usually only until the dependency which made it too costly is replaced.

At that point the root issue is rectified, and the associated risk mitigation activity and cost ceases.

They have sophisticated cost-modelling in place to know the cost curves of addressing risks strategically at source versus mitigating them operationally which make these decisions possible.

These mechanisms tend to be lacking in cybersecurity. When present they usually only look at optimising security operation costs, not the full value chain where the cause of the issue might be resolved permanently further upstream.

And on that note, I want to finish this section with a quick word on organisational structure:

Practitioners come to me in agreement with the above from time to time, but claim they have no choice as the source of a given problem originates in another part of the business over which they have no control.

My reply to this is that if a CISO (Chief Information Security Officer), a supposed C-level executive, doesn't have the ability to address the issues where they originate in order to deliver the best outcomes for the business due to a lack of organisational structure, authority, or influence, then establishing those things should be among the very first things they do.

If, in our plane analogy, it was a field technician who discovered the fault with the aircraft, that fault would be picked up by the manufacturer immediately and addressed as we discussed.

We wouldn't just let the field technicians retighten the fasteners forever and not take it further.

We know the best *overall* way of sorting the problem for the business is to escalate it and resolve it at source. As such, a structure has been put into place to make that possible.

Likewise, security cannot operate effectively in a silo and there is no excuse for it to remain there.

It is subject to the same need for a holistic approach and could learn an awful lot from other industries.

In fact, the best book I've ever read for achieving the highest possible security outcomes is The Toyota Way, by Jeffrey Liker.

Yes, a book about the Toyota Production System, a system that's been refined over decades with 14 principles on achieving the highest quality outputs with the greatest cost efficiency.

It is a better guide on how to structure an organisation to reach good security outcomes than the hundreds of cybersecurity books I've read in my career.

Why that focus on quality management is so important to achieve those security outcomes is what we're going to look at next.

3 – It's About Quality

The approach I just described could loosely be called "quality management".

The reason this quality management works so well in security (and why it's so extraordinary that we don't focus on it) is simple: security vulnerabilities, the very things that make us susceptible to attack, are virtually always quality issues, or defects.

Defects in code.

Defects in system builds.

Defects in operational procedures.

Defects in architecture.

Defects in process design.

Defects in lifecycle and maintenance cycle planning.

Defects in training.

Etc…

It is these defects that create the conditions that allow attackers to get systems [and people] to do unexpected things and gain control over our infrastructure and/or data.

Applying quality management principles gradually reduces the prevalence of such security-impacting defects over time. This means we have less and less exposure that needs managing.

Meanwhile, the security industry is incentivised by the number of vulnerabilities there are to mitigate with cybersecurity technology and services, not by solving the fundamental problems creating them.

Afterall, the issues and complexity must keep growing if today's security industry is to keep growing.

Since I mentioned "The Toyota Way" earlier, allow me to share an analogy about the security industry which I first devised arguing the "cybersecurity skills gap" which we'll discuss later in this booklet:

Imagine you're standing on the street looking at a car factory.

To one side is a huge parking lot, a staging ground for the finished cars to be shipped on for sale. On the other, the factory building itself.

An assembly line of a hundred or so stations puts together a finished car every few minutes which is then pushed out of the factory building into the parking lot.

Slight issue: we're pushing them out from the third floor.

The finished cars drop 25 feet into the lot, damaged, crumpled, and full of issues.

People rush towards them, flip them back onto their wheels, cart them to a corner of the lot, build a make-

shift workspace around them, assess the damage, figure out which parts need replacing, in what order things must be disassembled and reassembled to get to said parts, what tools we'll need, which issues to prioritise as there are so many, what the minimum level of repair is before we can send the cars off, and so forth.

The crumpled cars keep coming too, every few minutes another falls from the third floor of the factory.

The backlog and number of issues just keeps growing, so we hire more people, create specific subdisciplines, hire managers and governance experts to oversee it all, bring in vendors to sell us the latest tools and solutions, consultants to help with better methodologies for our repairs, auditors to make sure we meet our minimum standards, and so on.

Despite all this we must queue and prioritise, determine what's most important because we simply can't do it all.

The strain on finding qualified resources to do all this work is enormous too. And once found, retention and burnout are serious concerns.

This is, of course, absurd. But in the land of security operations this is normality.

The first time I told this analogy at a conference, without mentioning what it was about, the audience

started nodding and chuckling, recognising themselves.

It's no surprise that there's no time to identify the bigger problem. Most haven't even thought about it, or don't want to. They love this stuff, remember? Heck, the struggle is often seen as a badge of honour.

We, as businesses, can't keep going on like this though, we can't keep supporting this approach.

Quality management matters, not just to reduce risk, but to do so in a sustainable and cumulative fashion. It's the only way to keep the costs of security from rising exponentially over time.

And yes, dropping the cars off the 3rd floor is hyperbole. A better way of thinking about it is that issues are being introduced throughout the assembly line and resulting in many defects that need sorting at the end.

The defects we find in the car park are telling us what to fix on the assembly line, but it shouldn't end there either. Just like Toyota, we should continue to ask "why" even after we get an initial answer.

Because the process issue in a specific assembly station could be caused by yet something else that will continue to introduce process issues elsewhere if unresolved, and there may be yet another issue behind that.

The further upstream we go, the more issues we prevent.

4 – It's Not an IT Thing

Expanding on our earlier ship analogy, it's important to point out that information security isn't limited to IT or the IT department.

I once spoke to the Head of Infrastructure at a client's, an airport. One clever thing he told was how the luggage conveyor belts never break down.

This is achieved by having a sensor that tracks the voltage on every motor powering the conveyor belt. Should the voltage get erratic on one of these motors then that is a sign that it may soon fail and so it is replaced overnight outside of operating hours.

Brilliant.

A few more questions about the who and how reveals that the monitoring of these sensors is performed by an outside maintenance company, with no cybersecurity credentials whatsoever, through a direct connection to the airport's internal airside network behind the firewall.

Did the security team know that there was a direct outside connection bypassing a small fortune in network security? Unsurprisingly, they did not.

The Police Services of Northern Ireland had a huge data leak of tens of thousands of police officers' home addresses due to a poorly thought-out Freedom of Information process.

Uber lost millions of driver records due to a process in its legal department involving fax machines.

There was even a cybersecurity firm which was breached when their helpdesk gave an unauthorised person credentials.

In my experience, the majority of Security functions aren't even aware of the processes of their IT service desk, which gives access and credentials all day long, let alone what goes on in other departments.

How can they be expected to secure a whole organisation? They can't, not as an IT function.

You can't secure an organisation as though it was a computer, no matter how hard you try, and it's why I feel like we're seeing more and more breaches originate outside of the core IT function.

This is a critical part of what I call the fish tank problem.

There is a big misconception that removing X number or percentage of your technical vulnerabilities is an X level of decrease in risk.

This simply isn't the case due to the nature of security versus most functional things.

Imagine I order a one metre pane of glass. When it arrives, it turns out to only be 99 centimetres.

I bolt on some legs as my goal is to make a coffee table.

My table is 99cm instead of 100cm, but arguably just as functional. It's doing what I need it to do, I'm getting value out of it, and the difference is so small it's likely to go unnoticed. I've lost, at most, 1% of the functionality.

Now imagine I need the same pane of glass for the bottom of my aquarium. The difference in outcome from the missing centimetre is going to be enormous. I am going to lose a lot more than 1% of the water, I'm going to lose all of it. It's useless.

Now rather than a 1cm gap, imagine the bottom pane has holes in it, 100 of them. In this case you could argue that 99% of the assurance comes from the last 1% of coverage, because until you plug that last hole the eventual outcome is the same.

If you consider that most organisations don't even know about 10-20% of their *IT* assets (yes, this is a thing!), let alone what goes on in other departments, the odds of most organisations even getting close to 99% is slim.

In short, if there is a way around your controls, any gap at all, chances are the threats will be able to undermine all of them and get in.

As we said in our ship analogy, a holistic approach is key. *Any* gap will result in ingress.

It's therefore crucial for security to not be limited to the IT department, let alone a portion of the IT department. It must know about every part of every business process.

And yet, most Security functions know worryingly little about data and processes in Sales, Marketing, Finance, Legal, Engineering, etc.

This is why it's so important that your Security function not be a silo, and that your security programme be based not one some third-party technical or management standard as is so often the case but rather on the specific structure, details, circumstances, and systems of *your* business.

What a security programme or framework should do in my opinion is systematically go through your business processes as to be aware of all the risks you carry and, where feasible, help reshape them to prevent as many of those risks as possible from even existing.

Thereby driving that quality holistically so that there are fewer and fewer gaps, while being *wholly* aware of where today's gaps are.

More on this later.

5 – Strategic Use of Tools

It might sound like I'm advocating against all the cyber security tools out there, but I'm not.

In fact, I think they're incredibly good at helping us find the sources of the quality defects that we need to address. In the next section we'll talk about how they can even help us find *business* efficiencies we would never have identified otherwise!

The problem I have with security tools is that they're rarely if ever leveraged to achieve this, instead being used to manage the symptoms of our real problems.

Consider the example of a common security tool: the vulnerability scanner.

One of these will scan the computer systems on your network and report back any known vulnerabilities that it finds such as missing patches and known misconfigurations.

Imagine it finds about 10,000 of these across your organisation's network. This is not an unusual amount for a mid-sized organisation, but it's a number that's too high for the Security team to handle.

Fortunately, most of these vulnerabilities are categorised as of low, medium, high, or critical importance, and further broken down by whether they are on an internet-facing system where it could be readily exploited by anyone at large, and even

whether that vulnerability is known to currently be actively exploited.

This allows security practitioners to "strategically" prioritise the, say, 1,000 most important vulnerabilities. Those that are critical (which usually translates to easy to exploit), facing the internet, and for which we know hackers have the tools to exploit.

Sounds clever, and from an operational point it's a good way of prioritising seeing as we have limited resource and can't address everything.

But if we take a step back and apply some of the concepts presented so far, we quickly see that this isn't "strategic" at all: no one is asking why they have these vulnerabilities at in the first place.

Why do the software engineering practices result in the software vulnerabilities? Why are there processes resulting in systems that can't be patched? Why do the patching processes miss so many systems? How did systems get released or end up with bad configurations? Why are there systems not under management? Why have systems bypassed our build standards?

People in security when seeing the report, tend to see 10,000 individual vulnerabilities. They don't typically read between the lines, by which I mean they don't group them by *cause*.

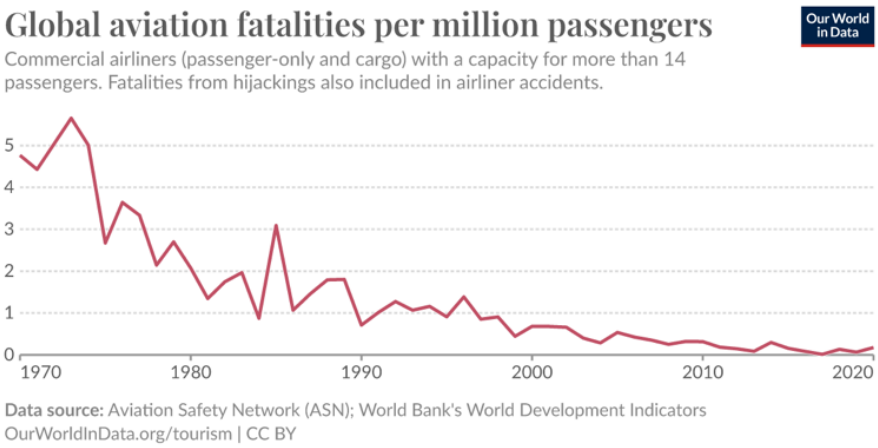
If we did, we would start seeing a handful of business or IT process issues causing the bulk of them. We'd find, for example, that 30% of our vulnerabilities are

due to bad engineering practices, 20% are due to an inadequate patching process, another 10% due to shadow IT caused by procurement and provisioning issues, and so forth.

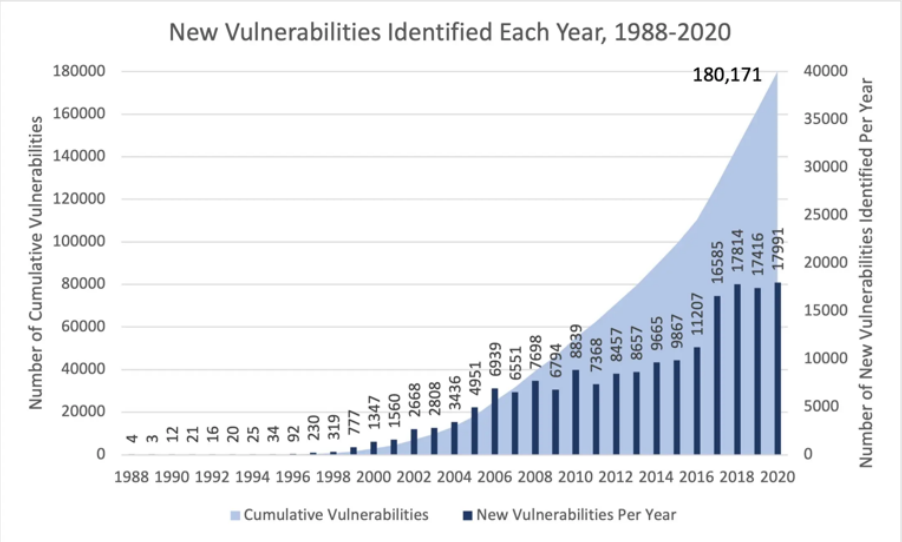
If, instead of just addressing the worst of the symptoms, we addressed the handful of business and IT processes *causing* them, then we won't have another 10,000 issues next year, adding up to the 9,000 we had left over from last year, and the hypothetical other 9,000 from the year before.

Instead, we'll have, say, 6,000 because we'll have resolved the causes behind 4,000 of them. If we keep repeating this process, the year after we'll have fewer still, and so on and so forth.

That way, our number of vulnerabilities over time goes down following a trend very similar to the graph we saw earlier showing the number of incidents over time in mature industries:



Compare that to the trends in cybersecurity:



It just gets worse and worse because we're too busy fighting the symptoms to even realise the real problem is elsewhere.

Furthermore, I would argue that we should be evaluating the severity of the causes behind our vulnerabilities rather than just the resulting symptoms if we're to prioritise things properly.

For example, a missing patch of very low criticality which most would argue isn't even worth addressing could be a symptom of a *very* serious process issue that next time around could produce something devastating.

Earlier this year, the head of a Vulnerability Management programme contacted me after he'd read my last book. He told me it made him realise that he'd spent the last decade burning himself out

playing whack-a-mole and that he now saw the real problem.

It's beautifully simple once we step away from the tech myopathy and start thinking about the big picture. As an executive used to doing just that, I bet this makes perfect sense to you.

The above was just a of example of what we can infer with a Vulnerability Management tool specifically, but all kinds of security tools have the potential to be leveraged in the same way.

The findings of an Identity Management solution can help you trace back issues in HR or role assignment processes, an Asset Discovery solution can help you identify issues in provisioning or procurement process, an Application Security solution can help you spot bad engineering practices, and so forth.

It can even lead us to business efficiencies that have nothing to do with security and which, ironically, might be security's biggest contribution to the bottom line yet. More on that in the next section.

I want to quickly mention another benefit of addressing things at the root cause: it also improves the likelihood of us catching incidents in the areas we *haven't* addressed yet.

That's because when we address the root causes of a certain type of issue, we stop that *type* of issue happening.

As a result, we don't just have fewer vulnerabilities streaming through, we have fewer *kinds* of them. That means fewer distinct things that need looking out for and less chance our security operations will miss them.

You might recognise a Batak machine:

It has a dozen spread-out circles which light up at random. You must continuously scan for one lighting up and tap it as quickly as possible.

Now imagine if only the three middle circles ever lit up. You'd be a lot less likely to miss one than if you'd constantly have to be looking all over, wouldn't you?

Personally, if my life depended on hitting every lit circle, I'd much prefer only having to worry about three of them. And I'd keep working to bring that number down further if I could.

6 – The Missed Business Value of Security

Why do businesses employ security? What's the point? What's the *value*?

Traditionally it's been about managing technical risks to reduce the annualised loss expectancy from those risks.

A security function therefore had to be able to reduce risk to a tangible degree so that the net benefit to the bottom line was greater than its cost. Something I'm not sure is often the case, if we could even measure it.

By addressing issues at source through quality management approaches instead, we amplify this equation by decreasing both the risks introduced and the costs to mitigate.

But there's more to be had from this. *Much more*.

Think about this for a moment: as mentioned earlier, every security issue is fundamentally a quality issue, *but not every quality issue is a security issue.*

For example, you might have software being produced which contains security vulnerabilities due to poor coding or testing. A clear security issue.

However, you may have software that's merely slow, maybe unstable. An annoyance, not great for customers, but not necessarily a security risk.

The kicker is that these problems often share the same root causes. In this case it might be poor software development practices behind both.

When it comes to technology, we often just assume things are the way they are without understanding underlying complexities.

If we want applications to run faster, we buy faster hardware. We don't consider that it might actually be our code that's slow due to low quality levels.

By chasing down the root causes of the security issues that our security tools find, we can often find and fix non-security problems as well. Problems we frequently didn't even have on the radar.

Let me give you a scenario where going after the root causes of security issues addressed significant issues the company wasn't aware of, and which made a real difference to the bottom line:

A SaaS business had an Engineering function that was producing an *enormous* number of vulnerabilities due to their practices.

Rather than spend a huge amount of money on compensating controls and application security testing to detect and send back dangerous issues, a different path was chosen.

After convincing the CEO that these issues were fundamentally engineering quality and not "security" issues, the organisation changed the leadership of the Engineering department, brought in a handful of

senior engineers to teach the team what good looked like, and got rid of the worst offenders.

Without going down the routes the security industry would advocate, the number of vulnerabilities in the applications dropped by 85% within a year. An improvement the typical security approaches would have struggled to achieve.

A perfect example of how we are best served by having Security influence IT and business process as to not introduce risk in the first place.

Not only was there no additional money spent on security solutions or approaches, but we *gave back* £200k in security OPEX due to the workload reduction. Even the overall Engineering cost fell slightly due to optimised headcount.

Then the really good stuff:

Product development sped up.

Applications ran noticeably faster.

Applications were more stable resulting in fewer support tickets and less rework.

Customers were happier with the platform, renewal rates increased.

Because the codebase was now more manageable and understandable, it became possible to develop features for customers (chargeable).

Internal users were happier too, and their productivity increased.

Site Reliability Engineers who were impossible to retain and costing a small fortune in recurring recruitment fees were no longer leaving due to their frustration at maintaining the platform.

The big one? Due to the platform being better architected and scaling more efficiently, the cloud computing costs fell by almost 30%. That's millions.

And so, with one initiative, a security team had a tangible ROI more than 200% of their annual budget *before* even calculating in the risk reduction.

This is the real value of security as a quality function.

It's not just about doing security more cost-effectively and sustainably by going after root causes.

It's that addressing those root causes can unlock a significant number of efficiencies that may have gone unnoticed otherwise. Efficiencies that can bring dramatic savings and opportunities throughout the business.

Beware the Myths

Now that you've absorbed the concepts in the previous six sections (I once again recommend going over them a second time as even more will fall into place), I want to quickly share my thoughts on a few hot cybersecurity topics.

Topics which I think you'll now be able to appreciate with a fresh and more critical perspective.

I've singled these out as you're likely to have heard of them. They are some of the biggest "arguments" being pushed on companies by parts the security industry to justify significant spending.

It's important for you to understand these arguments (or "myths") and why they may not hold water in some situations so that you are not misled and are able to make the correct decisions for your organisation.

So, without further ado, let's have a quick reality check around certifications, the threat landscape, and the supposed "cybersecurity skills gap".

Certified Secure

The first "myth" I want to raise is the idea that certifications make organisations secure. This is rarely the case.

They focus on generic and academic views of technology, not your specific implementations or how they align to your business, people, what you use them for, etc.

As we've discussed, fit is extremely important and security is a whole-business thing, not an IT sub-function.

An effective security programme needs to reflect your organisation by going through all your departments and business processes (including IT) and eliminate sources of risk by defining what good looks like *for you*. No canned outside standard can do this.

What risks can't be process-engineered out can then at least be comprehensively inventoried, so you know what needs mitigation (beyond the IT silo too).

This is the best way of preventing as much as possible, and the *only* way to be sure of capturing all remaining risks.

In my opinion most certification processes also fail to provide real assurance due to the approach in accrediting and auditing.

In school you would get a test that covered maybe 2% of a book. But you didn't know which 2%, so you had to read through and study the whole book.

Most certifications work the other way around, showing you the questions first, so you only end up going through the 2% of the book you need to pass.

They're also a point in time, usually with lapses between audits. In the real world you're tested on 100% of the book, *all of the time*.

When I audited breached organisations on behalf of cyberinsurance companies, it was my job to show they were negligent so the policy wouldn't need to be paid out. It was often this tick box approach and the disconnect between some third-party standard and their specific business reality that made this task easy for me.

It should be mentioned that having a certification on paper in no way excuses any financial or even criminal liability when something goes wrong. This is a curiously common misconception.

Consider also that the reasons behind the demand or companies to have these accreditations, not to mention mandatory regulations in certain sectors, is in part because of the failures which have forced industries and regulators to put on the pressure.

But the more we focalise on compliance over practical security outcomes, the more failures there will be and the greater the regulatory pressure (and costs) will likely become.

The only way to reverse this tide in my opinion is to start delivering the outcome of security so that the regulatory pressures to do better subside.

This way we should see fewer new regulations and may see a relaxation of current ones as we demonstrate that success is achieved differently.

What I suggest to customers is to build a programme or framework that is bespoke to their organisation. This doesn't just provide better protection but is also easier to maintain as it reflects their specific reality.

Such a bespoke programme or framework can then be quickly mapped to third party standards.

This makes it possible to meet the obligations of new regulated locales and industries in weeks rather than months or years, which can give a significant competitive advantage in the form of business agility.

In summary, our highest obligation of compliance should be to what we have defined as the ideal state for our business. Only afterwards should we map that back to third-party standards or requirements.

Who's Feeding the Mice?

The second "myth" I want to bring up is about the "threat ecosystem."

It's likely the single biggest thing vendors and consultancies use to push the sale of cybersecurity products and services.

I can't deny that it has evolved and grown into something of a scale and sophistication that is hard to fathom. There are thousands of organised groups, some with hundreds of members and affiliates, lone hackers, fraudsters, even nation states.

It's pretty scary, really.

But we are ignoring how we got here, and how these ecosystems continue to grow. We are ignoring that it's us that's enabling them, fuelling them.

They are enabled by the vulnerabilities in our systems and organisations and, as we discussed earlier, we have far too many of these – almost all avoidable if we'd focused more on their root causes.

Think of it this way: if you were to dump a big canvas bag of seeds in your garden, would you be surprised to have hundreds of mice a week later?

I doubt it.

But how would you deal with it? Leave the seeds and buy hundreds of mousetraps?

A source of food with traps around it will still attract those mice, it's inevitable some will get through, it's a big capital investment, and will require constant maintenance.

A better approach would be to store the seeds elsewhere, or in a metal tin.

An even better one might be to not bring in the seeds until we start planting so we don't need to store them at all, which also saves us effort and money (a perfect example of how a clever and streamlined process can reduce both costs and risks).

In short, it's us who are providing the threat ecosystem everything it needs to grow, and the mousetrap market has little interest in changing how we operate.

Rather than keep attracting and try to fend off the threats, we should be thinking about how not to attract them and eventually starve them out. It's the only way we're going to make a dent in this problem.

Next time a security vendor tries to scare you into buying mousetraps, think about why you might have so many seeds available to the mice in the first place, you might even find an opportunity to save some money.

The threats are out of our control, but our environments and processes aren't. So why wouldn't we focus on the things we can control rather than spend time and effort on what we can't?

In 1987, a British ferry departed Zeebrugge in Belgium. Moments later, it flooded with water and capsized, killing 193 people.

The investigation blamed a myriad of things:

- Leaving the port with the doors still open.
- The hand in charge of operating the door being asleep.
- A lack of process checks.
- A lack of alarms.
- A lack of compartmentalisation of the ship.
- Poor communication.
- A lax company culture.

Do you know what they didn't blame?

The water.

Let's focus on building better boats, not trying to fight off the ocean.

The Cybersecurity Skills Gap

Our third “myth” is about one of the biggest costs of doing cybersecurity: headcount.

Cybersecurity roles are largely demanding and often stressful, with significant salaries. Worse still, there are not enough qualified candidates available, and turnover is high.

It’s simply the nature of a field focused on gruelling firefighting, complex technology, and constant risk.

But what if, instead of hiring and trying to attract and retain these costly technical experts, we took a different path to achieve security that was less reliant on them?

Afterall, isn’t a route that makes us dependent on scarce and expensive resource a bad strategy element by itself?

In my last CISO role I hired a team so “unqualified” that I was deemed reckless by some industry peers. People actually wrote to my employer to express their concern about what I was doing. I was even called unethical.

An entire team put in place in two weeks, off the back of a LinkedIn post. No HR, no recruiters, with a budget I was told simply could not hire good people.

I hired a former teacher, policeman, sales manager, IT architect, former air hostess turned business

owner, and an aviation technician. Most of them had never worked in dedicated cybersecurity roles before.

This may sound odd, but that is *why* I hired them.

Remember the car factory analogy?

Well, these misfits sat in that figurative parking lot watching people swarming all over those broken cars, intimidated by all the complex tasks they saw going on. They probably wondered what I'd gotten them into, and whether their new boss was crazy.

After a while they mustered up the courage to ask me a stupid question that none of the expensive cyber experts I *should* have hired would have:

"Why are we dropping the cars from the third floor?"

Because they weren't indoctrinated techies, the real problem was obvious to them. They had the common sense and communication skills to go drive change on the assembly line. They cared more about the outcome than how you're supposed to "do security".

The impact that team made to the security posture and costs of that business dwarfed what a technical team twice the size could have achieved.

How many of the thousands of cybersecurity roles that you'll find on job boards involve actually looking at how the *business* operates and identifying where issues come from?

It's essentially zero.

I'm not saying we don't need any of the techies, of course we do. But if we don't solve the underlying problems, we'll need an infinity of them. Hence the current shortage.

They must be led by people who think about what's best for the business and how we will achieve outcomes rather than chase more technology.

I believe this lack of vision, leadership, and strategy is the real "skills gap" in cybersecurity.

As most executives are well aware, a good leader, a good strategist, a good visionary can make an enormous difference.

Yet in security these things are sometimes actually frowned upon by many technology elitists.

There's more too. As we mentioned in the "That's Not Security" section, many security organisations don't have much of a strategy besides just buying and implementing more tools.

Without a strategy, how do they even know what people to hire as to achieve the desired outcomes?

They don't. They hire people to operate and manage tools, putting the job market under ever-more pressure.

We can do better.

Commercialising Security

So far, we've looked at how approaching security as a quality management function not only improves our long-term security posture but also reduces our relative security costs, especially over time.

Even more significantly for the bottom line, we've seen how addressing security in this way can lead us to find previously unseen inefficiencies in business and IT processes.

These can generate very significant savings, especially in technical areas but often in others such as Sales, HR, and Legal as well,

But what if, in addition to these savings, we generated *revenue* from our security efforts as well?

Let's have a look at what that might look like and how a commercially minded CISO can help not just defeat cyber threats, but your competitors as well.

A Better Garage

I own a lovely classic car that I cherish, but I struggle to trust garages for its maintenance due to a series of bad experiences with work being done poorly, or not done at all, which has left me suspicious.

One day I heard good things about a new garage and decided to give them a try.

Right away I noticed there was a level of information and transparency in their reception area that I wasn't used to. They even have a big window in the back that let me see into the workshop.

Through it I could see them working on my car, with care, doing everything they said they would.

When I got my bill, it listed all the same things the bill from the last garage did. The difference is that in that garage I couldn't see the work, and therefore I couldn't trust the work.

This new garage is a little more expensive, but it's where I'll be coming back to. The peace of mind is worth it.

Cybersecurity has some parallels to this because much of it happens behind closed doors and it's hard to know what's actually being done, and whether it's being done well.

I once looked into a managed monitoring service that had been commissioned by the Security function of a new employer. It was costing us £23,600 per month.

Unfortunately, due to poor contract review, they failed to note that the service exceptions covered the *entirety* of the contract.

That's right. The provider had done precisely *nothing*, and they were perfectly within their right to do so.

This had been going on for 42 months.

Nothing had been checked, and just shy of £1 million had been paid. For nothing.

When uncovered, the embarrassment to the security function was so great that the CISO sacked me for bringing it to light.

Even worse, this managed service was part of a contractual agreement the company had with its largest customer, putting it in breach of contract.

I wish I could say that this kind of thing was uncommon, but I can't. In fact, it was far from the first occurrence at that company, just the one with the biggest price tag.

Things like this fuel my distrust in companies when it comes to security. But what if we used the lack of transparency by others to our advantage?

In my last CISO role, my company received a tender request from a major strategic client. They wanted to see what our new SaaS platform could deliver compared to our competitors.

The questions were all functional, there was nothing about security. That would all be handled later by the "security people" with their checklists and questionnaires. No one really cared about that stuff.

The SaaS functionality we were being asked about involved this company, a global enterprise with a market capitalisation of about one hundred billion dollars, sharing some significant intellectual property with whoever was going to win the tender.

No one at the customer seemed to have considered the possible risks to their business caused by sharing that information with third parties like us.

I think most companies in our position would rather not mention that using them introduced such risks.

We did the opposite.

In our reply deck, my team added some slides which showed our assessment of the customer's risks, what it could mean to them, and how we'd structured security across our development lifecycle, platform, and organisation to address those risks.

They hadn't asked, but we answered anyway.

By making the customer aware of the risk(s) they were taking, we created an interest in security. We made them realise security should be a *primary* requirement in their selection process.

As a result, they would start asking our competitors more pointed questions about capabilities in an area where we were sure we could beat them.

We knew our competitors likely didn't have a programme that was as business-aligned as ours, that had thought about the customer's risks, their data, their potential business impacts, had answers ready, even created polished security materials for them.

The best our competitors could muster would probably be an ISO 27001 certificate or similar. It was unlikely that they had materials, or had thought beyond technology, or would be willing to be transparent about the state of their infrastructure the way we could.

These are things that normally get little commercial consideration and are kept out of sight of customers.

We instead gave it focus and gravitas, positioning it so that alarm bells went off in the customer's mind when our competitors didn't.

We were against much bigger and more established competitors in that tender. We were the upstart at a significant disadvantage in a conservative market.

We won.

Branding Security

Giving confidence in your security can yield significant commercial results in end-consumer situations too.

I'll spare you the full story because it's a long one, but years ago the American retail chain Target started using data from its customer loyalty programme to predict when customers were pregnant.

Sometimes before those customers knew it themselves!

Pregnant women are, for obvious reasons, a goldmine for a store like Target. Diapers, food, safety items, car seats, clothes, swings, toys, strollers, etc.

Plus, while you're in the store for baby things you may as well buy yourself that new set of cookware, that new coffee table, a fresh bed set, and that big TV you wanted.

Target kept deepening that advantage by learning more and more about their customers as they shopped.

This fed a positive spiral where they could learn about and cater to their specific needs. Knowing everything from what sized clothing they wore, what gender they were, toys they might like, when potty training was likely to happen, religious occasions, birthdays, what sports they played, school preparations, proms, etc.

And as that child grew up going to Target with its parents for just about everything, they even created a whole new generation of customers.

It could do this because it had customer insights to shape its marketing efforts to *devastating* effect.

But customers today are becoming reticent about sharing their information due to an awareness of breaches becoming more common.

It's therefore increasingly important to not just have good security but also to communicate it as part of our brand. Only by providing consumers with sufficient peace of mind will they share with us the data we need to maximise our competitive advantage.

In some verticals, the difference between getting their data and not can be the difference between a striving business and a struggling one.

Caring about customers' data also communicates that we care about *them*. That by itself is a powerful psychological motivator (the reciprocity effect) that can drive them to want to do business with *us*.

Businesses have invested a lot of money into security, but security usually does little to return the favour commercially.

A commercial security strategy that supports your business goals is an opportunity not to be wasted.

Parting Words

That brings us to the end of this booklet.

We opened with a quote from Drew Simonis, who recently had more to say while commenting on a LinkedIn post. It seems a fitting bookend:

"There is momentum in treating the symptoms our approach has led to. People have jobs they understand, the business has expectations they are comfortable with, leaders have certain beliefs about what a good strategy is, vendors have whole businesses based on it. An entire shadow industry exists to train people [on] how to participate in the broken system.

Momentum like this is hard to overcome. But I'm with you. Time to change is long past. We need to hit the reset button and be ready to realise, as Pogo says: 'We have met the enemy, and he is us.'"

I trust you now understand what he meant by this.

And I hope that you too now agree that the concepts and approaches discussed here make more sense in overcoming our challenges, while also providing more value to you and your business.

It's a journey you need to be taking, and we'd like to help.

About Sequoia Consulting

If you hadn't read this booklet and I'd told you we dealt in cybersecurity, I'm fairly sure you would have had a very different idea in your head about what we do than what was presented here.

When rebranding to our current motto, "Obsessed With the Bottom Line", I posted a few other options on LinkedIn.

One of these was "Putting the Business First." I was advised against it by several people.

Why? Because they felt "putting the business first" might be threatening to security practitioners.

Let that sink in.

That is why we are adamant about *not* being a "cybersecurity" company. While we work *with* Security functions, we do not typically work *for* them.

Think of us more as a management consultancy that looks at your problems holistically in order to find the absolute best operating model and results for your business.

Yes, we ensure security functions are accountable and operationally effective through well-defined process, but that's only the first step.

We help you implement everything you need to leverage the concepts presented in this booklet, continuously reducing your risks and risk mitigation costs by defining what good should look like throughout your organisation.

By doing so we also identify and fix hidden business issues to further improve the health of your organisation and its bottom line.

It's interesting to note that large consultancies like McKinsey, KPMG, Boston Consulting Group, etc., historically have very sophisticated methodologies to understand your unique business and provide the right answers for your specific situation.

And yet, when it comes to cybersecurity, those same consultancies push one-size fits all approaches that largely neglect your underlying business reality.

That's where we come in. We assess, perform business process inventory, develop strategy, and then the programmes and roadmaps to reach your ideal outcome.

When it comes to getting the most out of security, we have no doubt that our initial Orange Peel Assessment, so called because it begins to peel back the skin of your unique situation, is the single best investment you can make.

You'll find our typical approach detailed on our website: https://www.sequoia-consulting.co.uk

Also on the website, you'll find our manifesto, about which I'm proud the Head of Risk Management (EMEA) of the second largest investment bank in the world had this to say:

"*[I] love the underlaying basis of these statements - which should resonate with many security purists that have too much love for the problem to understand the inadequacy of their solutions.*"

Our role is to help your organisations establish the vision, strategy, and structure to achieve the *outcome* of security in a way that maximises the benefit to your bottom line. That's it.

I look forward to hearing from you.

Sincerely,

Greg van der Gaast

Managing Director
Sequoia Consulting and Advisory Ltd.

SEQUOIA CONSULTING

Obsessed With the Bottom Line

“The significant problems we face cannot be solved at the same level of thinking we were at when we created them.”

-Albert Einstein

Security spending has been growing for over twenty years now, yet risks continue to increase exponentially. The unsustainability is undeniable.

Security is not fundamentally complicated. It has been made to seem that way by an industry that thrives on mitigating issues through technology but often has little interest in resolving their causes.

This booklet aims to help non-technical executives see past the hype of “cyber” and identify and address the underlying business problems responsible for our current situation - which the security industry largely fails to address.

"[I] love the underlaying basis of these statements - which should resonate with many security purists that have too much love for the problem to understand the inadequacy of their solutions."

-Calin Gheorghiu, Head of Risk Assessment & Advisory [EMEA] at a top 3 global financial institution, upon reading our manifesto putting business outcomes ahead of security "solutions".

Read it for yourself at www.sequoia-consulting.co.uk/manifesto

Reviews of the author's previous books:

"Every Information Security professional needs to read this."
"Hits the nail right on the head. Should be required reading."
"The best infosec book I have read."
"I've lost count of the amount of times I've recounted things Greg said to my customers and left them in awe."

Greg van der Gaast

Greg started his career by hacking a nuclear weapons facility and then working covertly for the US Government. Despite this, due to an obsession with pursuing root causes in order to achieve outcomes rather than just "do security", his perspective on security is arguably less technical, more holistic and, above all, more business-focused than the status quo.

He is a passionate advocate for the industry to stop pushing a confusing and siloed technology-first discipline, adopt accountability, and generate results. After working as a CISO for a number of years, he's now Managing Director of Sequoia Consulting where he helps clients achieve business outcomes by improving the quality of business and IT process rather than just fighting the resulting fires with "cyber" technology.

SEQUOIA CONSULTING

Obsessed With the Bottom Line