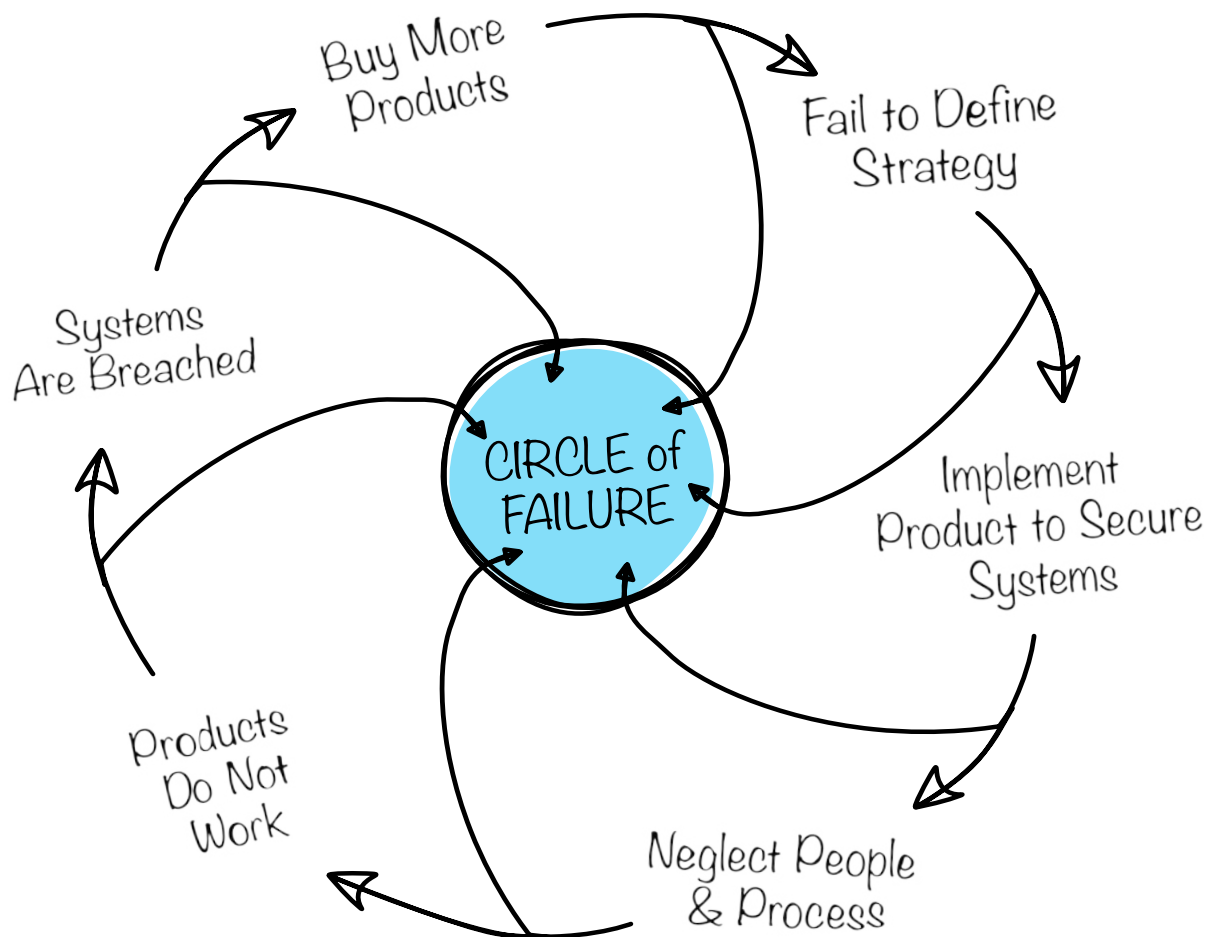


THE CIRCLE OF FAILURE

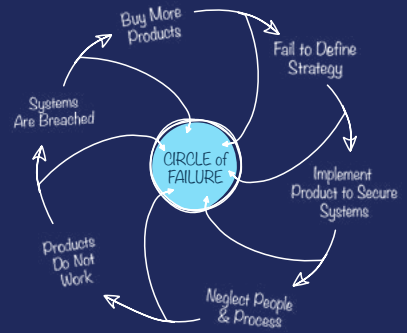
Why the Cyber Security Industry Doesn't Work



CONTENTS

- 1 The Failure of Our Industry**
- 4 The Failures of Our Product Vendors**
- 9 The Failures of Our Managed Security Service Providers**
- 14 The Failures of Our Internet Service Providers**
- 18 The Failures of Our Businesses**
- 23 Our Biggest Failure**
- 24 What You Can Do About It**
- 25 The Change Checklist**
- 26 The Product Vendor Checklist**
- 27 The Service Provider Checklist**
- 29 Risk Crew - Who We Are**

The Failure of Our Industry



The cyber security industry has failed. The evidence is clearly visible and overwhelmingly, everywhere. If you agree that the cyber security (our industry) was founded on the fundamental objective of preventing information technology systems from breaches and data theft, then you must surely agree that it has failed us. If you don't agree, then you are not paying attention.

It has been over 35 years since the first computer virus was reported, back in 1986. In 2019, the World Economic Forum added; cyber attacks, data fraud and information theft to their top ten list of long terms risks considered; most likely to occur, most impactful should they occur and most concerning for businesses globally.

So, after more than three decades of practice, 30% of the top ten list of global risks are now attributed to the cyber security industry – the risks our industry was (and is) professionally responsible for addressing. Our industry has failed.

The evidence is overwhelming. If you don't agree, then you are not paying attention.

The Regulation

The first clear sign of our failure was the onset of legislation and regulation like the Health Insurance Portability and Accountability Act (HIPAA), the European Union's Cyber Security Directive, and Security of Network and Information Systems (NIS Directive), the General Data Protection Regulation (GDPR) and the United Kingdom Data Protection Act 2018.

When the government gets involved, it's because the industry has failed. Similar to the massive safety regulations mandated on the energy, automotive and airline industries in the 1970s.

The increase in this type of legislation and regulation is a direct corollary to our failure to protect our systems and the data we process, store and transmit.

The Breaches

The indisputable proof must be the breach statistics. Our industry currently recognisesⁱ that there are:

18,525,816 records are compromised every day

771,909 records are compromised every hour

12,865 records are compromised every minute

214 records are compromised every second

HACKED

The Records Lost

Look at those numbers. We are losing over 18 million records every dayⁱⁱ. The number of personal records lost by companies that should know how to protect them is staggering:

Yahoo: 3.0b

Facebook: 533m

Marriot International: 500m

LinkedIn: 700m

River City Media: 1.4b

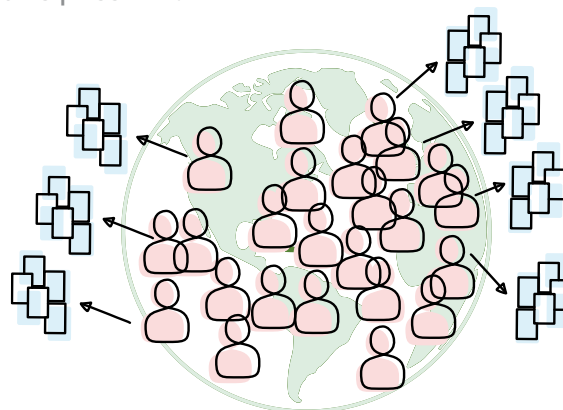
Aadhaar: 1.1b

First American Corporation: 885m

SpamBot: 711m

Syniverse: 500m

We have lost over 14 billion records just in the last seven years aloneⁱⁱⁱ and that's just those reported from countries with mandatory disclosure legislation. That's more than twice the number of people walking on the face of this planet. How is this possible?

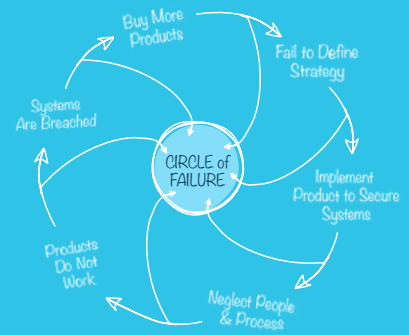


The breaches and regulations clearly show that we are not getting the job done. We are failing.

Why? What are the root causes of this failure? Is our industry inherently designed to fail?

Let's start with the obvious.

The Failures of Our Product Vendors



Our product vendors have failed our industry. Why?

Because their products simply DO NOT WORK. Say it aloud and you'll feel better. Cyber security products don't work. They do not meet the challenges presented by the threats in our industry – they never have. That's a fact.

The products are, and have always been, reactive – not proactive.

Our product vendors have failed to keep pace with the skills, ingenuity, and adaptability of the threat actors our industry faces. They are a step behind the threats when clearly, their job is to be a step ahead.

They have failed to do this. Consequently, the threat actors have set the pace of the game and we cannot keep up.



Our vendors sell us knives to take to gunfights.

The Hype & FUD

Vendors in every industry hype their products. This is understandable and expected. But the hyperbole in our industry is second to none.

Our vendors wrap their products in marketing messages cloaked in such ambiguous jargon and superfluous buzzwords that their actual role and effectiveness is undecipherable – and that of course is exactly the point.

Hype-as-a-Service (HaaS). Where would our industry be without it?

And of course, there's the fear. Fear, Uncertainty and Doubt (FUD). We are told to: "Be afraid." "Be very afraid." Fear fuels the content of every vendor website, blog, podcast, webinar, social media post, product overview and conference presentation found in our industry. It's clearly depicted in the imagery with the industry's use of face-less hoody-wearing hackers hunched in shadows, staring at monitors, emblazoned with skulls and crossbones. "Be afraid." "Be very afraid."

So, we are, and this fear clouds our judgement. This is the objective of using it. FUD is a proven wartime propaganda strategy. It's "us against them." Fear them. Trust us. We can protect you from them. The more FUD is repeated, the more it enters the collective unconscious and the greater its effect is on us as buyers.

The result is that we base cyber security strategies on FUD – and NOT on what is good for our businesses.

FUD



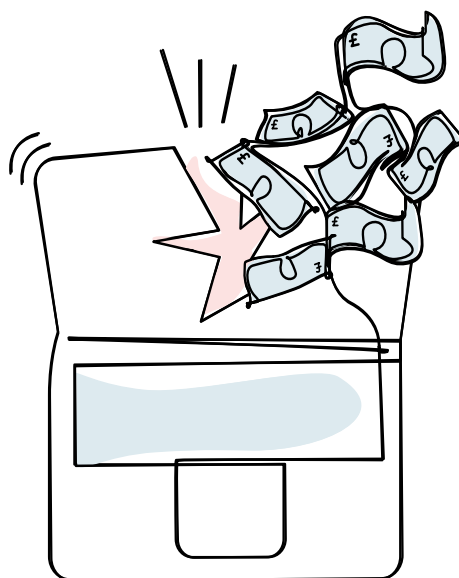
FUD is the enemy. "What you need to secure your business systems is our: quantum, next generation, global network edge-based, on-premises, hyper automated, unified extended reality cyber security mesh. Which, by the way, we can also offer as-a-Service (aaS)."

The Un\$spoken Oxymoron

To understand the role that vendors play in our industry, we must start to acknowledge the unspoken oxymoron: Computer security vendors profit from the insecurity of computing.

The fact is that we look to our vendors to solve our cyber security problems but fail to recognise that it's not in their long-term economic best interest to do so.

Like the pharmaceutical industry that profits from treating sicknesses, colds, flu, diseases, viruses, and infections, we are an industry wherein our vendors also find their profit from treating the symptoms rather than finding the cure.



Our vendors focus on treating the wounds, viruses and infections because this is where the money is.



Have you noticed that every major cyber security attack from Operation Shady RAT, World of Hell, Red October, WannaCry, Not WannaCry and Petya, were followed by significant profit and share increases for the leading vendors in the industry? Why is that?

How is it that our cyber security vendors profit from breaches and not by preventing them?



The answer is obvious. Businesses buy the products to secure their systems. The products do not work so they get breached. The breaches scare businesses into buying more products. The products do not work, so breaches continue... It's a revenue cycle that perpetuates itself. Why would they stop it if they profit from it?

The Accountability Blackhole

Accountability is the foundation of every business transaction made. Sellers are accountable to buyers to deliver on their promises. Simple.

For organisations, vendor accountability is the approach they take to confirm the performance and results of the products and services purchased from their vendors. For vendors, on the other hand, accountability is being responsible for decisions made or not made, actions taken or not, and results achieved or not for the buyers of their product. It's taking full responsibility to do what it takes to achieve what is agreed with the buyer. Not so simple and conspicuously absent in the cyber security industry.

Unlike other industries, cyber security product vendors are not held accountable in the event that their products do not work.



For instance, if malware is undetected by an anti-malware product, the vendor is not responsible. If traffic gets through a firewall that should prohibit it, the vendor is not responsible. If an intrusion detection system does not identify an intrusion, the vendor is not responsible.

Product specifications and Service Level Agreements (SLAs) in the cyber security industry are specifically worded to ensure that the vendor bears zero liability in the event their product does not perform as expected or its performance (or lack thereof) is associated with a breach. Why is that acceptable? Isn't that the very reason we buy the product? If you bought a parachute and it did not work – wouldn't you hold the vendor accountable?

Without vendor accountability, why would we expect products that work?

The Leadership Void

Look at this list of vendors who are the leaders in our industry. We go to them to buy the products to secure our systems but do note that everyone on this list has been hacked in the last 18 months^{iv} – and of course many, many others. These are the “leaders.” These are the “trusted names.” The vendors we look to for leadership. They talk the talk – but they do not “walk the walk.”

We buy products from these vendors to solve our problems when in fact they are struggling to solve the same problems that we are. These are not shepherds, they are sheep.

When SonicWall’s Secure Remote Access solution product line got hacked last year, they released a press statement that blamed it on a 0-day vulnerability that inadvertently provided a “backdoor” to attackers.

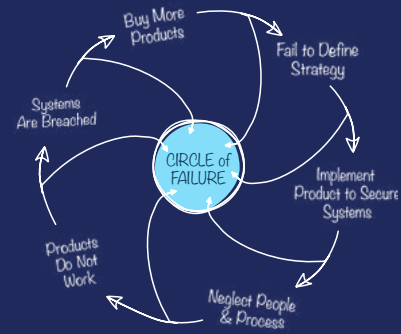
If the definition of a 0-day vulnerability is an unknown coding error (or an “unknown unknown”), ask yourself, how is it that a vendor can have an “unknown” anything in a product they manufactured? How is it that a vendor can produce software code with a backdoor to it and not know it?

Every day we are finding more and more backdoors, exploitable vulnerabilities, and inherent design deficiencies in the security products we trust – and bought to protect our systems. It seems that cyber security vendors do not practice “secure by design” principles. The irony should be apparent to us all.

RSA
FireEye
F-Secure
iSight
Tenable
ThreatConnect
ThreatTrack
SonicWall
Novetta
Symantec
AVAST
Bit9
Verisign

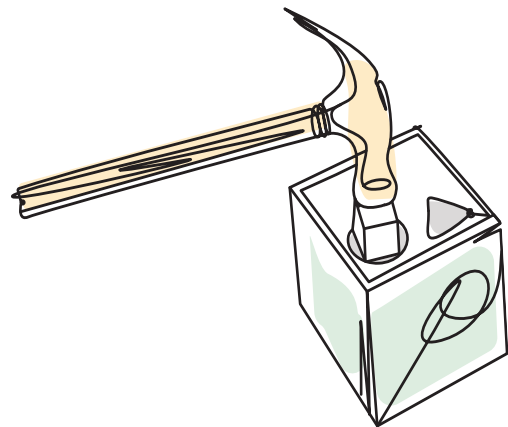
Leaders should lead by example. However, there’s a clear and distinct lack of leadership in the cyber security industry.

The Failures of Our Managed Security Service Providers



Managed Security Service Providers (MSSPs) have also failed us but in a different way than our vendors. Vendors sell us products. MSSPs technically are selling us a process – *a product-centric process*, but a process, nonetheless. We buy monitoring, management or reporting solutions from our MSSPs but these “solutions” have failed us. Failure is inherent in their design.

Why? Because these services are based on their product’s capabilities and not our specific business requirements. They are not based on our actual business practices and processes. But to a vendor with a hammer – everything looks like a nail.



MSSPs provide packaged solutions that are **easy for them** to deploy but **difficult for us** to integrate into our systems, leaving big holes in coverage. These gaps in coverage leave us more vulnerable to cyber threats than before we bought and installed the product.

The obvious example is that they do not cover Software as a Service (SaaS) or other non-traditional platforms. Do you know of a business that does not have an information asset in a SaaS platform like Salesforce, GitHub or Dropbox? What’s the point of a security information and event management service that can’t identify an intrusion or data exfiltration associated with a SaaS platform?

The irrelevance of the majority of MSSP solutions was clearly demonstrated in the SolarWinds attack. At best, these solutions are designed to address the problems we faced 20 years ago. They are useless in today’s threat landscape, much less tomorrow’s.

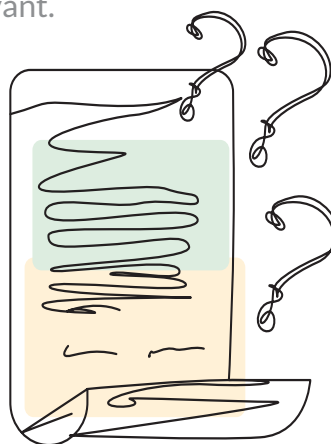
The Mysterious Case of the Ambiguous Maintenance & Management Agreement

In addition to their failure to fully integrate their solutions into our systems, MSSP service level agreements lack clearly defined procedures and responsibilities for the ongoing maintenance and management of these tools. By the very nature of what they do (or are supposed to do), these tools must be finely tuned and continuously managed and maintained to keep them effective.

The data points monitored by these tools are driven by the vendor's configuration. Poor configuration results in poor coverage and of course produces poor findings. What is monitored and reported can quickly become irrelevant.

Have you ever read an SLA for a typical MSSP solution?

It's never clear what the MSSP is responsible for and what the customer must take on themselves until long after the solution is deployed... if even then.



In the meantime, you assume the MSSP has the wheel, while they assume that you're driving. It takes a breach for us to read the SLA and then of course, it's too late. This is no mistake. MSSP service level agreements are designed to be vague. They wouldn't have it any other way.

The “False Positive” Paradox

But the biggest failure is that MSSP solutions produce such enormous amounts of false positives. There’s a clever marketing term – “false positive.” If a false positive is an alert that incorrectly indicates a vulnerability is present, why don’t we call them “false alerts” – because that’s what they are?

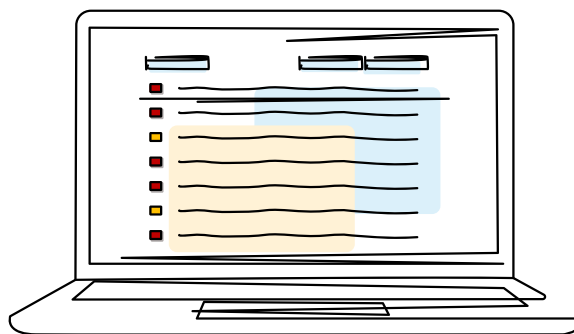
Any alert without context is typically reported as a false positive. It doesn’t mean it’s a vulnerability. It also doesn’t mean it’s **not** a vulnerability. It only means that it requires investigation to resolve it. To be clear, it means that you must investigate and resolve it – not the MSSP.

Given that the industry currently recognises that 40% of SIEM alerts^v are false positives, this creates significant work that few of us have the time or expertise to address.

These solutions are like smoke detectors with weak batteries – with every beep, the onus is on **you** to investigate and assess the smoke for signs of an actual fire. We don’t need smoke detectors – we need flame detectors and qualified firefighters to put out the fire.

What happens next is exactly what you would expect. We are overwhelmed with false alarms and so naturally succumb to “alert fatigue.”

Consequently, over 30% of security staff typically ignore up to 50% of SIEM alerts.^{vi}



While the algorithm required to differentiate false positives from true positives is no doubt difficult for a MSSP to write, when your product is wrong 40% of the time, maybe, just maybe, you’re not ready for market.

The paradox is why we keep buying them.

The Absence of Accountability

Just like cyber security product vendors, our MSSPs go to great lengths to ensure that they are not held liable if their monitoring solutions do not work. If a vulnerability goes undetected, is exploited, and then results in a breach of our systems – they bear absolutely no responsibility.

Solution specifications and SLAs are expressly worded to ensure that the service provider bears zero accountability if their solution does not perform as expected or its performance (or lack thereof) is associated with a breach.

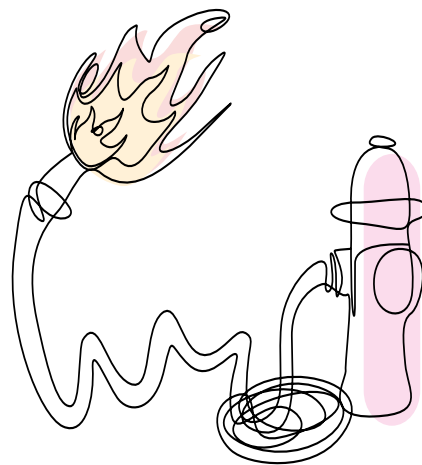
Again, why is that acceptable to us? Isn't that the very reason we buy the service – to detect a vulnerability that could result in a breach?

If you bought a fire prevention system and it failed to detect the fire that burned your house down, wouldn't the service provider bear some responsibility? Especially if they manufactured, installed configured and monitored it?

Solution specifications and SLAs are expressly worded to ensure that the service provider bears zero accountability if their solution does not perform as expected or its performance (or lack thereof) is associated with a breach.

If you bought a fire prevention system and it failed to detect the fire that burned your house down, wouldn't the service provider bear some responsibility?

Especially if they manufactured, installed configured and monitored it?



Without accountability, our houses will continue to burn down.

The Leadership Void Part II

These are the leading MSSPs in our industry. The providers we turn to for the solutions to monitor our systems for security vulnerabilities, incidents, events, anomalies and of course – breaches.

We look to these companies as subject matter experts who will help us secure our systems. Our industry professionals that we pay for their expertise. So naturally we look to them as the authorities on the cyber threat landscape, threat actors and vectors, targets, tools and attack methodologies.

It's ironic then that every MSSP on this list has also been hacked in the last 18 months.^{vii} Like our industry's product vendors, our MSSPs don't seem capable of securing their own systems. Don't they use their own products?

A leader is one who knows the way, shows the way, and goes the way.

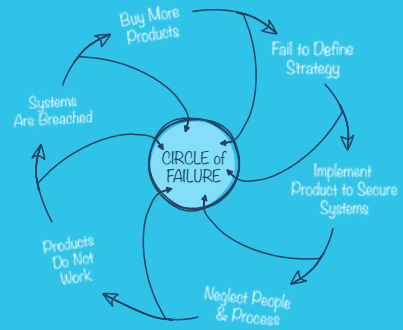
Why is it that we continue to purchase solutions from MSSPs who clearly do not “know the way?” Their directions are useless. They're as lost as we are, and yet we continue to pay them a monthly subscription fee to show us the way.

There's a distinct absence of leadership in our industry. Where are the vendors and service providers who lead by example?

A dark blue rectangular stamp with the word "HACKED" in white, bold, sans-serif capital letters. The stamp has a distressed, ink-like texture with some white noise and irregular edges.

Mimecast
Stormshield
Wind River
CISCO
NTT
Microsoft
Cognizant
Belden
Keepnet Labs
Imperva
Comodo
NordVPN

The Failures of Our Internet Service Providers



Our Internet Service Providers (ISPs) have failed us. ISPs provide the gateways we all use to access the Internet. As such, they are in a unique position of access control. They open the door to this crazy nightclub we call the Internet. We pay them the (monthly) cover charge and we're in. No questions asked.

But this is a rough club. There are no minimum entry requirements and once inside, there are no rules, no laws or no policing. No difference between right and wrong. No consequences for bad behaviour. On the Internet anything goes from identity theft to paedophilia. It's a tough place.

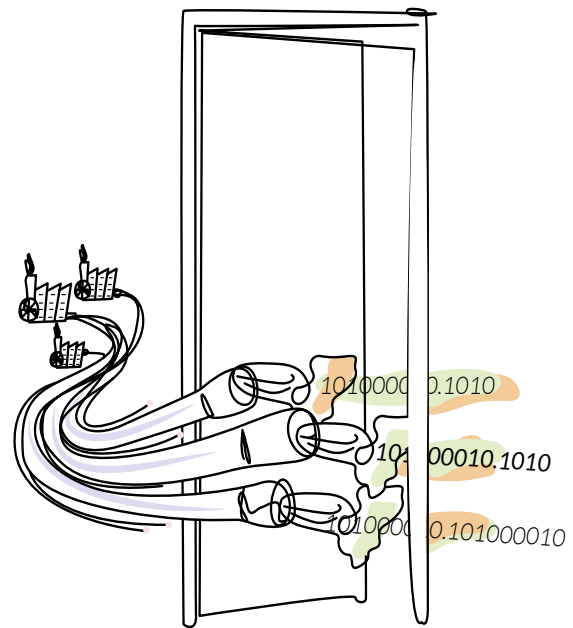
But maybe it's a tough place because our ISPs let anybody in the door. Why aren't they acting as bouncers to this club, denying access to clearly bad elements and throwing out anybody inside who's acting as a threat to the rest of us? This is not to advocate regulation – but just the implementation of some common sense and basic consumer safety measures. Our Internet Service Providers (ISPs) have failed us.

Think how different the Internet could look if the ISPs did a little housecleaning.

Why don't our ISPs provide or enforce any minimum-security controls for accessing their networks? Why don't they filter malware? Why can't they block bad sites and prevent IP spoofing? Why don't they report much less prosecute people who use their services to commit a crime? Think how different the Internet could be if suddenly ISPs did a little house cleaning, but they don't.

Why don't they stop the botnets or DDoS attacks that traverse their networks? Because its revenue, that's why. Because they sell bandwidth. They sell the bandwidth that the botnets and DDoS attacks consume. They sell the bandwidth that delivers the malware and phishing attacks to the front doors of our homes and businesses.

Security is not their revenue stream. Bandwidth is their revenue stream – at the expense of security.



This is understandable. They are in business to make money. But couldn't they find a revenue stream in providing secure Internet services? Wouldn't you pay more for an ISP that blocked phishing emails?

Our industry has missed an opportunity to enlist the help of the ISPs in our cyber security fight.



As a result, they have become part of the problem – rather than the solution.

ISP Accountability

(Insert joke here...)

It is not news that ISPs are not accountable for the behaviour of their users. They are not accountable for any of the content or traffic their networks carry. They are not accountable for breaches associated with their services. They are not accountable for damage to the devices and networks connected to their services. And of course, they are not accountable for any financial losses incurred by our households or businesses due to criminal activity committed through their services.

When it comes to security accountability – there's nothing to see here.
[Move along.](#)

The real news is, as consumers, that this doesn't bother us. We don't seem to care about this complete lack of accountability from a commercial provider that delivers what is nothing less than a critical service to our homes and businesses. Because the Internet is just that. It's a vital and essential part of our lives – like water and electricity. It's a utility.

If one of your utility providers damaged your home or business through their poor services, you'd hold them accountable, wouldn't you? And yet, we don't hold our ISPs accountable for delivering the ransomware that puts us out of business. Why not? Is this an unreasonable expectation? Where's the duty of care? Where are the best efforts? Where's the minimum effort?

Accountability is the glue that ties commitment to the result.

Without ISP accountability, why would we expect anything on the Internet threat landscape to significantly change anytime soon – or anytime at all for that matter?

Leaders Wanted – Apply Within

By now you can clearly see where this is going. This is a list of the leading ISPs in the industry and yes, every one of them has had their business infrastructures breached in the last 18 months^{viii}.

Like our industry's vendors and MSSPs, our ISPs seem unable to secure their own business infrastructures and unwilling to cleanse the threats from the Internet traffic they carry to and from our devices. They provide the pipes and claim no responsibility for the raw sewage these pipes deliver to our homes and businesses.

If there is any one single component in our industry that could make us all considerably more secure instantly – it is our Internet service providers.

They are in a unique position to be able to implement minor changes that would bring major benefits. By simply installing basic filters in these pipes, ISPs could dramatically clean the sewage we receive every time we log on.

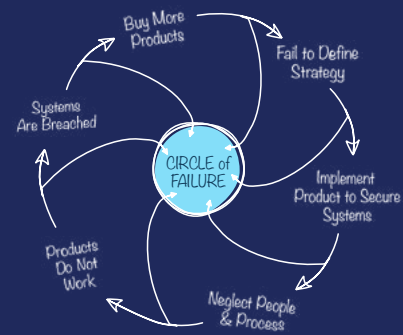
There is no question that cybercrime has reaped havoc on all of us and ISPs are the obvious candidates for taking the first steps to do something about it given its impact on their paying customers. That's clear. What is not clear, is why they are not stepping up and why that's ok with us.

A graphic of a white, distressed, stamp-like text "HACKED" on a dark blue background.

Comcast
Verizon
Draytek
A1 Telecom
Talk Talk
Sky
Virgin Media
Vodafone
BT
EE
PlusNet
PocketiNet

Leadership is about making others better.

The Failures of Our Businesses



Without question, our businesses have failed to meet the challenges of cyber security. Year after year, we attend conference after conference on how they are unable or unwilling to formulate or execute an effective cyber security strategy. The lucky few who have an approach are incapable of effectively communicating it to the board, stakeholders, and staff, so it is never fully realised.

Our businesses continually embrace new technology without consideration of its inherent security risks and are then shocked when the rollout of that new cool, money-saving, digital transformation to that next-gen platform is breached. Wireless, Cloud, IoT – they seem to have no collective memory. It's like our businesses have amnesia and déjà vu at the same time – they have forgotten all of this before.

Job titles, responsibilities and salaries have evolved from Information Technology Security Manager to Chief Information Security Officer and yet each year brings a record number of data breaches. We have tried “on-shore insourcing” and “off-shore outsourcing” and vice versa with no success.

Businesses of every model, size and sector have failed miserably when it comes to protecting the systems that process, store, and transmit the data they depend on for profit. Leadership failures? Of course. Lack of accountability? Certainly.

Our industry conference agendas are filled with presentation titles listing the ways our business have failed in meeting the challenges of cyber security. These failures that are shared by all businesses, are critical to understanding the problem and involve three fundamentals – the Maths, Execution and Moral.

The Maths Failure

First, businesses have yet to understand and quantify the clear cost benefits associated with good cyber security practices. They still struggle with simple maths like calculating mitigation ratios and sums for Annualised Loss Expectancies (ALE) necessary to determine the Return on Security Investments (ROSI) for their cyber security spend.

$$\text{ROSI (\%)} = \frac{\text{ALE * Mitigation Ratio} - \text{Cost of Solution}}{\text{Cost of Solution}}$$

Accurately calculated, ROSI provides actionable data needed to confirm that information security management programme activities actually support the business strategy and reduce cyber risks.

The data is essential in verifying whether security spend is justified and sufficient or grossly inadequate. It is critical in determining if resources should be reallocated and to what issues.

But after more than three decades of practice, we have yet to master this simple arithmetic and incorporate cyber security return into our business models. As a result, cyber security budgets lack specific focus and are either “guesstimated” or addressed ad hoc – either way they are not aligned to the strategy.

After more than three decades of practice, we have yet to master this simple arithmetic and incorporate cyber security return into our business models.



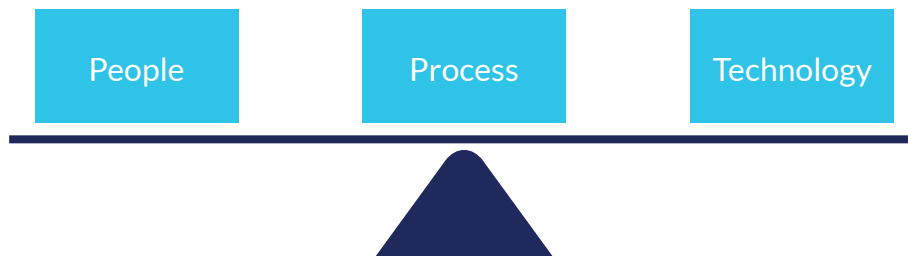
As a result, cyber security budgets lack specific focus and are either “guesstimated” or addressed ad hoc – either way they are not aligned to the strategy.

The Execution Failure

Second, businesses have failed to understand that cyber security is an oxymoron. Cyber security is risk management. Consequently, a cyber security strategy is one that identifies, minimises, and manages the risks to the information assets required to generate revenue. Most businesses have not identified these assets, much less quantified their actual value; and those who have failed to align their (limited) resources (to fully protect them).

If our industry experts have agreed on one thing, it's that the best cyber security strategy is a holistic one that incorporates people, process and technology.

This basic principle is found in all the learning objectives established for our professional certification courses. Protect all three attack vectors: people, process and technology – it is what every qualified industry professional has been taught. It's supposed to be our game plan.



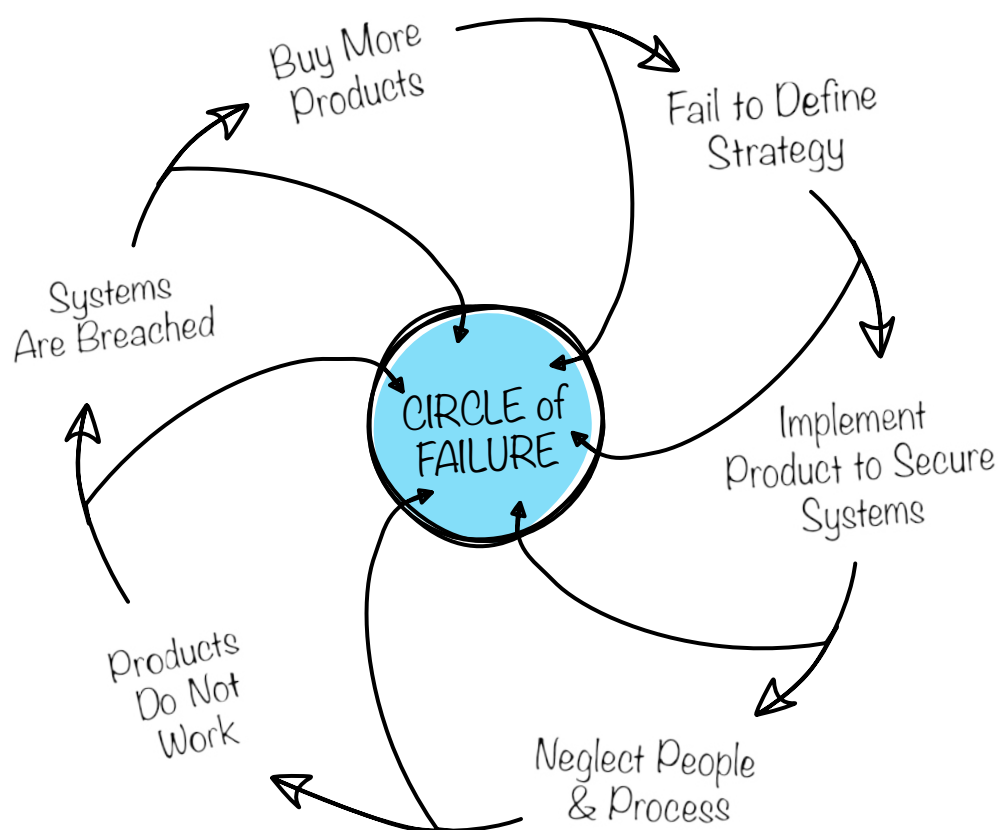
And yet, we fail to execute this game plan in our businesses. Have you ever seen an organisation that evenly allocates its cyber security budget across all three vectors?

For instance, have you seen any business that spends the same on security awareness training for their staff as they do on conducting security penetration testing of their systems?

The reasons for this failure are twofold. First, because of our inability to measure the ROSI associated with investing in people and process – cyber security gets delegated to the IT department and consequently, becomes subject to its culture and perpetual resource limitations.

As a result, cyber security is seen through the eyes of the IT department as a technology problem and they mistakenly implement product for a solution, a strategy enthusiastically supported by our industry's vendors.

The result is that businesses are caught in the Cyber Security Circle of Failure.



By neglecting two-thirds of the attack vectors used by threat actors and implementing security products that don't work to protect the business systems – we become trapped in a vicious circle of failure.

The Moral Failure

Finally, and maybe most disappointedly, our businesses have failed to recognise their moral obligation to safeguard the sensitive data entrusted to them by their employees and customers.

Businesses have approached data security as the challenge of safeguarding 1s and 0s. Placing financial data aside, our business systems process, store and transmit data about human beings.

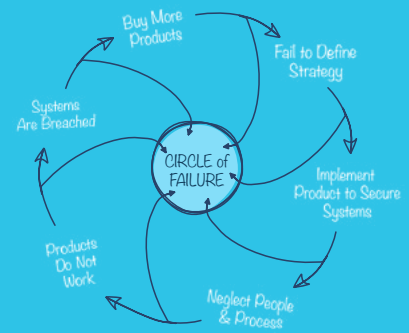
This is not about protecting 1s and 0s – this is about protecting data about people's lives. It is about protecting data, the data of someone's grandmother or grandfather, mother or father, husband or wife. This is about protecting data about someone's child. It's about protecting your data. It's about protecting my data.

Real people have suffered real consequences because businesses have failed to protect their data. Why have they not acknowledged this moral responsibility?

Businesses have a duty of care to do everything in their power to protect the data entrusted to them. When you give a business your personal data, don't you expect them to protect it? Of course, you do. The protection of your data is implied in the transaction, and it is the very least they should do in exchange for the privilege of your business. Would you give a business your data if you thought that they were not going to protect them? Of course, you wouldn't.

Businesses have failed to realise that cyber security is just the right thing to do.

Our Biggest Failure



Without question, the biggest failure in the cyber security industry today is – you. It’s me. It’s us. We are all collectively, the underlying cause for all the failures in our industry. As consumers, we are the reason that the cyber security industry does not work.

The cyber security industry doesn’t work because:

We believe what we are told

We do not demand value for our money

We do not expect more

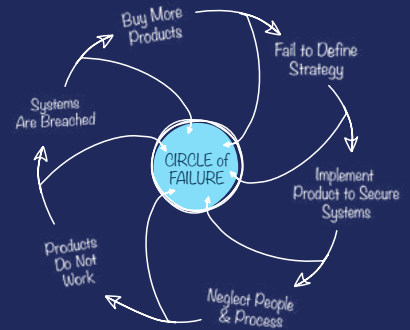
We do not ask for more

We do not hold anyone accountable for anything

Quite simply, the cyber security industry has failed us because we have failed it. We have failed to apply the same standard of excellence that we demand in all other areas of our lives to our industry.

Why is that? When we buy a product or service from any other industry, we expect it to work. If it didn’t live up to our expectations, we would demand our money back. Why is this not the practice in the cyber security industry? If we buy an anti-malware software solution and then get ransomware, why don’t we hold the vendor accountable for the inferior quality of their product? Until we do, we are the root cause of the failures of our industry.

What You Can Do About It



If you agree that our industry does not work and want to see change – then be the change you wish to see.

Do you know that there are currently over 4,000 enterprise-level cyber security products to choose from on the market? There are literally thousands of MSSPs and ISPs out there to choose from. All these vendors and service providers are vying for your dollar, pound, euro or yen. Can you imagine the change that you could affect in our industry if, as a consumer of those products and services, tomorrow you started expecting more? Then next week – you started demanding more?

Exercise your power as a consumer. Expect more. Demand more. And maybe, just maybe, you might just get it.

Do not think that you cannot make a difference. The change begins with you.
Start now by using the change checklist.

The Change Checklist

Here are ten things you can do now to start to bring about real change in our industry and break the Cyber Security Circle of Failure:

Say this aloud: “Cyber security is a process not a product.” Repeat, as necessary.

The enemy is FUD. Remove it from your thinking. Base your cyber security strategy and purchases solely on what’s good for the business. Nothing else matters.

Confirm your cyber security budget is equally allocated in thirds to address vulnerabilities across people, process and technology attack vectors.

Calculate the ROSI for every cyber security expenditure – every single last one.

Up your game and request that the Board and Senior Management store their personal and financial details on the business system. If it’s not secure enough for their sensitive data, it’s not secure enough for your fellow employees, partners and customers.

Identify KPIs for products that would confirm that they are supporting your risk management goals and objectives – before purchase.

Hold your vendors accountable for the products you buy from them. If they fail, ask for your money back. Repeat, as necessary.

Purchase only those MSSP solutions that support your business processes – not the providers.

Identify KPIs for MSSP solutions that would confirm that they are supporting your organisation’s risk management goals and objectives – before purchase.

Hold your service providers accountable for the services you buy from them. If they fail, ask for your money back. Repeat, as necessary.

Product Vendor Checklist

When you buy a product ask the vendor:



Was the product subject to “secure by design” principles and practices during development? If so, which, and will you provide evidence?



Has the product been subject to security testing? If so, what kind and will you provide evidence?



Does your company use the product? If so, how and will you provide evidence and a point of contact I can speak with?



Has your company been breached in the last five years? If so, what role did this product play in that breach?



Does the product provide remote connectivity to your company or any third parties? If so, will you provide details to include your liability in the event of a breach of this connectivity?



Will you provide details on the company ownership and supply chain for this product for purposes of a risk assessment?



Will you install and configure the product to ensure it works to my satisfaction?



Will you manage and maintain the product to my satisfaction? If so, for how long?



Will you train my staff to understand the product’s performance requirements to my satisfaction? If so, for how long?



What is your liability in the event your product fails?




What is your liability in the event that your product is determined to be the source of a breach to your systems?





Will you provide ten customers’ references?


Managed Service Provider Checklist


When you buy a managed service, ask the provider:

 Does your company use the service? If so, will you provide evidence and a point of contact I can speak with?


 Does your company also sell post breach services? If so, does your company generate the majority of its revenue selling its monitoring and preventative services or its post breach services?

 Has your company been breached in the last five years? If so, what role did this service play in that breach?


 Does the service provide remote connectivity to any other third parties? If so, will you provide details to include your liability in the event of a breach associated with this connectivity?


 Will you provide details on the company ownership and supply chain for this service for purposes of a risk assessment?

 Will you install and configure the service to ensure it works to my satisfaction?

 Will you train my staff to understand the product's performance requirements to my satisfaction? If so, for how long?

 Are incident response services included in this solution?

 Are service components subject to routine vulnerability assessment scanning and security penetration testing? If so, will you provide evidence?

 Were service software components subject to secure development procedures and testing? If so, will you provide evidence?

 Are service components subject to regular security patching? If so, will you provide evidence?



Will you remediate any alerts you generate?



Will you provide active noise filtration and alert management to reduce false positives and support effective issue resolution?



Are alerts the only way you measure the security state of my environment?



What is your liability in the event your service fails?



What is your liability in the event that your service is determined to be the source of a breach to your systems?



Will you provide ten customers' references?

References:

- i Breached Records More Than Doubled in H1 2018, Reveals Breach Level Index - Thales blog ([thalesgroup.com](https://www.thalesgroup.com))
- ii Open Source 2022
- iii The World in Data Breaches ([varonis.com](https://www.varonis.com))
- iv U.S. State Data Breach Lists (iapp.org)
- v Ponemon Institute Survey 2018
- vi Ponemon Institute Survey 2018
- vii The World in Data Breaches ([varonis.com](https://www.varonis.com))
- viii The Word in Data Breaches ([varonis.com](https://www.varonis.com))

Risk Crew

Who We Are

Risk Crew is a London-based, product-agnostic information security governance risk, compliance, and testing consultancy. Crew members are chosen for their vision, innovative thinking and facility to embrace change.

We approach every project with our unique methodology:



Think Deeply

We take nothing for granted and think beyond current beliefs, preconceived ideas and prevailing opinions.



Question Assumptions

We do not assume answers to problems, we verify them.



Detect Cause & Effect

We confirm the relationship between events to confirm the source of a problem.



Deliver Pragmatic & Measurable Results

We include (KPIs) key performance indicators in our solutions to confirm their ongoing effectiveness. By questioning all assumptions, thinking deeply, detecting cause and effect, the crew delivers pragmatic, measurable results.

Get in touch and put us to work for you

+44 (0) 20 3653 1234

riskcrew.com

info@riskcrew.com

5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom

