KnowBe4
Human error. Conquered.

WHITEPAPER

The Department of No!

by Javvad Malik

Table of Contents

The Organisation-Security Relationship 3
What Does the Data Say? 3
What the Experts Say 4
Building the Security Brand 9
Conclusion 10

Security teams have a reputation—perhaps deserved—for being a barrier to progress.

They're the overly-cautious ones. While everyone else sees silver linings, they're pointing out the threatening clouds within them. If they have a signature word, it's: "no."

Does marketing want to share some behavioral insights with a new partner? That's a "no" from the CISO, even if it will bring in seven figures of business. Need to deploy a new business-critical application within the next week? Not without a pentest, says the security department. Oh, and they're booked for the next six months.

You can understand why others tend to perceive them as a blockage. But that's just part of the story.

Contemporary information security departments have evolved. What started as a murky corner of the basement-bound IT team has grown to encompass a broader swathe of disciplines: white hats, strategists, educators, regulators and so on. These various forms of evolution have ultimately transformed the role altogether.

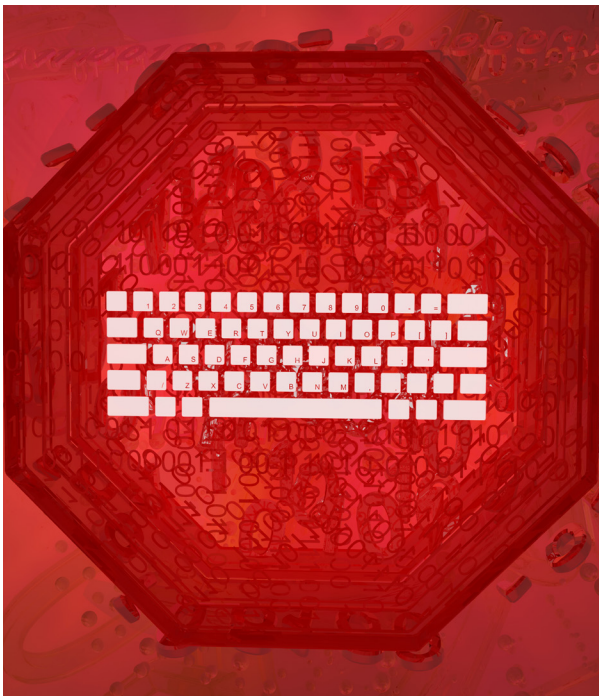
Security is no longer exclusively concerned with password hygiene and document management. It's now regarded as an integral part of a business. Security has earned its seat at the conference table, and the shiny corner office that ensues. And yet, that reputation for being the department that says "no" persists.

This prevailing reputation is not necessarily a good thing. While there's always room for cautiousness, being excessively so can be harmful, cause damaging workplace cohesion, and encourage employees to circumvent existing rules. This trepidation can come from a desire to work faster, to work without being bogged down in (often necessary) bureaucracy, or from a fear of being reprimanded.

Not every CISO or security team has fallen into this trap. In some organisations, they've managed to market themselves as an indispensable asset. A department or person to work with, rather than fight against.

This report will take a closer look at the habits of successful security teams and the secret sauce that makes them work. These methodologies they've deployed could work for your organisation, transforming the perception of your security team from blockade to vital partner.

The Organisation-Security Relationship



Brad Pitt and Angelina Jolie. Kate Moss and Pete Doherty. And yes, security departments and literally everyone else in the organisation. These are all pairings known for their often-turbulent relationships. And just like the glistening showbiz world, infosec teams often go through the full cycle of relationship drama—turmoil, highs and lows, and even occasional breakups.

But where does the fault line originate? Attributing blame—be that to a security department or a colleague—isn't always straightforward, because this remains somewhat of a taboo topic seldom discussed in the disinfecting light of day.

My first port of call was ex-CISO Thom Langford, who echoed that sentiment exactly. "It's difficult to say," he said. "Nobody would admit it."

Langford went on to describe a real example of a security team earning the unenviable moniker of the "Department of No."

> *"A former predecessor fell into this category," he said. "I was regaled multiple times of the cases where she literally stopped a business in its tracks until they just ignored her."*

Of course, some factors influence the path a security team chooses to take. Shan Lee, CISO at fintech titan Transferwise, pointed out that the size and type of organisation play a role in shaping a security team's perception.

> *"I think the bigger/older/more heavily regulated the business is, the more true that [IT teams are regarded as the "Department of No"] is," he said. "My team has an unwritten rule that we never say no, we offer alternative routes. We also have a lot of informal 'drop-ins' on Zoom, where anyone can ask about an idea they've had before it becomes an actual project, and no questions are stupid."*

Of course, for every story of collaborative and healthy security-colleague relations, there are hundreds more of "shadow IT" leaking into an organisation, and valued employees potentially getting disciplined as a result.

What Does the Data Say?

Let's go beyond the anecdotes. CLTRe, a KnowBe4 company, has pointed a beady eye at security culture across 24 countries. Their latest survey looks at data from 120,050 employees working across 1107 organisations to understand their relationship with IT in general.

Nearly 70% of respondents said that IT support was available, should they encounter a problem, with only 20% reporting "limited availability." Shockingly, 11% said that IT support was completely unavailable, and they were entirely on their own, should they encounter a problem.

There is a stark industry split here. Just 63.9% of those in banking, for example, reported having access to IT support. That is less than those in the retail and wholesale industry, where 66.7% responded in the affirmative. For legal industry workers, that number soared to 68%.

A smaller number—but at 62%, still a majority—reported having an awareness of company security policies. A further 24% reported limited awareness, while 13% claimed to be completely oblivious to the business's security policies. That means they are potentially unaware of corporate rules about handling incoming email attachments, using personal devices for work or accessing business systems securely.

We see a similar industry split here, with those in highly regulated industries (like financial services and legal services) reporting a higher awareness than those in lesser-regulated sectors, like retail and construction.

Fortunately, there is an overall better understanding of reporting security issues, with 79% of respondents describing their workplace reporting process as "clear." Just 14% said the rules were "vague," with 7% saying they are "unclear." While that's not necessarily indicative of a healthy colleague-security relationship, it does show that some feel comfortable in reporting potential issues—like a spear phishing email or an unknown individual walking unescorted through the premises—up the chain of command.

Motivation, however, is a problem, with just 57% describing that efforts to maintain security have been rewarded. Nine percent said their work was "unrewarded," while 34% said they were "neither rewarded nor unrewarded"—implying their compliance was otherwise unrecognised.

What the Experts Say

I set out to gain insights from a few security experts in the industry who have directly or indirectly been involved in building or branding security departments.

Ed Tucker, former CISO at HMRC firmly believes that marketing, and particularly security awareness activities, are best led by those outside of the security department.

> *"I'm starting to come to the conclusion that security people should not be involved in security awareness activities at all. Why is almost everyone so awful at it? Engage with your comms teams and let them lead. That's going to be hard and frustrating, but let them lead. They do comms. Let them lead!"*

Tucker added some tips on how to engage your comms teams, along with some choice words for fellow security professionals.

> *"Ask them to remove almost all security language in its entirety. It's a language that we use, not [with] the people you're trying to engage. You're going to hate it, but seriously step back!*
>
> *And if this is really frustrating because the comms people 'don't get it,' it's down to your inability to explain it to them in a way they do understand.*
>
> *Can you see the little problem here in you doing it yourself?*
>
> *One other tip that I personally have found useful is to engage with online safety educators. These people make a living from educating real human beings; children, parents, teachers, families, you know, your customers. Your employees are customers of yours BTW.*
>
> *Too much security is done from the position of prejudice of being a security professional, peer reviewed by security (with same prejudice) and just passed out. The lack of engagement and influence from business functions / areas / expertise into everything security does is such a blocker to successful outcomes. We have failed time and again to be business-led and use business leaders' expertise in our understanding and execution of things that are ultimately for them and directly affect them.*
>
> *Policy is a great one. We are largely terrible at it. Look at security policies in almost any org. Badly written, no sense of business knowledge or engagement, out of date, and largely ignored or progress inhibiting. Why don't we engage people who are actually good at this stuff who reside in the business to help us, both in engagement and in formulating and writing these policies to make them even vaguely relevant and readable.*
>
> *Maybe we're scared to admit we're not good at it? I don't know. Or fail to look outwards to find people with expertise to help. Whatever the blocker is, we're not doing it, which makes our policies, as this example, suboptimal."*

"One other tip that I personally have found useful is to engage with online safety educators. These people make a living from educating real human beings; children, parents, teachers, families, you know, your customers. Your employees are customers of yours BTW."

Rowenna Fielding, senior data protection lead, adding to Tucker's comments, emphasised that culture plays a considerable role in communications. She cites diversity as a much-needed component in tech as a whole.

> *I'm also going to note that women are socialised to be better communicators (both by expectations of others and as a defence mechanism), but sexist men won't listen to women and there's a *lot* of sexism in tech… still.*
>
> *My point being that crap comms is an emergent property of the infosec culture and demographic makeup. As such, there are multiple factors which need to be tweaked to produce a different outcome. Diversity is a very, very important one.*
>
> *And by that, I mean diversity of background, culture, race, gender, sexuality, physicality, and opinion. Not for 'political correctness,' or 'virtue signaling' or all those bad-faith interpretations, but to break open the echo chamber!*
>
> *Infosec culture teaches infosec people to hold themselves above the rest of humanity, with superior knowledge and skills, protecting the 'users' for their own good (yes; not all, etc.—but most, too many, etc). People as seen as exploitable assets/vulnerable liabilities.*
>
> *There's not much room there for the empathy and humility required to be an effective educator in order to develop.*
>
> *Framing infosec in terms of conflict, with militarised analogies and confrontational language—not conducive to fostering a spirit of collaboration. Definitely not helpful to dealing with the degrees of subtlety and nuance that infosec requires.*
>
> *In techie terms; for full-duplex communication to take place successfully, all nodes need to be equipped with a common set of protocols and languages.*
>
> *But here's the thing—you can't just install your preferred protocol stack on another human being with the click of a button. Nope, humans don't work that way.*
>
> *You have to build a common set of references with every node. By the way, there is huge variance in components, operating systems, applications and configuration between nodes; but they are all critical, in their own way, to the overall architecture.*
>
> *In summary, comms between people are not client-server operations, no single human is the right tool for all the jobs, and monoculture is self-defeating."*

Human risk and security culture expert Mo Amin agreed that the "department of no" label was justified in many cases.

> *"Unfortunately, the evidence bears it out. Especially in larger and older organisations and less so in start ups and more agile-led environments. Naturally, an established company typically has had a few negative experiences with their security function and there's some trust debt. However, I do see positive signs of improvement. It's a slow process but it is getting better.*

Build your security function as a service, consumerise it. Ways of working have changed. Security functions need to be agile in approach and delivery.

I asked Amin to share some of his experiences of security teams that do the right thing to which he shared this list:

Typically:

- If they have to say no, they are able to offer an alternative, unless the risk is too great. They are able to defend their "No's".
- An engagement first approach. Where they take a collaborative approach with transparent communication.
- Those who build security as a service.
- Those who have clear, context-specific and easy-to-find guidance.
- Those who empower and enable the business—where they understand a business unit/team's pain points and work to minimise them.
- Where they have security champions/ambassadors—that are trained, and a feedback loop to the security function exists. They use that feedback to continuously improve.
- What things could they do better to improve their image with the organisation and having a positive impact on employees?
- Less an "us vs. them" attitude, have an "ask us anything" attitude. Be open and approachable.
- Provide security tips and guidance that staff can use at home.
- Trust and confidence build brands—make sure you deliver on what you say you will. If you can't, you need to be able to defend it.
- When security functions say "security is everyone's responsibility" but don't make it easy for people to take that responsibility—where practically possible remove as much friction as possible.
- Build your security function as a service, consumerise it. Ways of working have changed. Security functions need to be agile in approach and delivery.

Krishan Tank, BISO, believes security teams have moved on from the "Department of No" label.

> *"From my perspective, sec teams have moved from 'no' to 'yes,' and this is how you do it safely. [It is] much more collaborative and gives you a standing invite to meetings as you're not getting in the way of progress."*

Where sec functions fall down (large enterprise ones) is [when] they decide on a program of work and essentially dish it out to the BU or CTO function to comply with. That doesn't get the full support, even if those functions recognise the value. Partnering also means partnerships on garnering input before you release a program of work and understand the impact on the BU/CTO (i.e. it's usually the same product operations team dealing with the scanning results, pen test results, security audits, service outages, product delivery support and incident management). Security needs to be mindful of what else other functions have on their plate, acknowledge and support, but still impress the wider picture of enterprise security.

My role particularly looks at how to navigate the numerous services the enterprise function provides and sell that to the business knowing it's a maze, and often people have no idea about what that service is!"

Andy Rose, CSO at Vocalink, also disagreed with characterising security functions as the "Department of No."

No. Hasn't been for 10-15+ years in my experience. I left my first major security role because of that issue as I saw the technical staff avoiding security and doing what they wanted without involving us, as they knew my leaders would say no. It made security much worse.

I did experience it at a major firm too—the acting security manager realised that staff could surf porn from their company-issued mobile devices as it didn't go through the internet filter—so he blocked internet access… unbelievable! It did, however, lead to them headhunting me to 'sort out security.'

The teams now have to be focused on business outcomes and enabling business development and growth. The answer now is always "yes, and here's one way we could do that".

Security has to identify where folks are not keeping to policy and use that, not as a stick to beat the employees, but as an indicator of a constrained process or technology. People using WhatsApp? Why isn't your internal comms good enough—what is the gap—how can security enable the internal tool to be better? People using Dropbox? What internal file sharing capabilities have you provided—can they work with external parties—how can they be made easier to use (and remain secure)?

Make employees understand that security has an impact on the business and on them. Ensure they know the right thing to do, then monitor what they actually do and look for lessons to be learned! Staff will ALWAYS find the most efficient way for their process (like water downhill), so learn from that, and then design security around those established ways of working, only standing in their way when there is a damned good reason.

Get involved in the CTO technology roadmap discussions—see what tech the CTO is interested in and get ahead by investigating the associated risks and possible solutions.

Make staff realise the risk associated with technology and then the simple things that we can do to protect them. Use their home computing equipment as an example.

As ever, it's a people problem. Make sure the control creates as little disruption as possible and enables useful working practices, and then ensure that staff know WHY the control is essential.

Building the Security Brand

The data suggests that things aren't as dire as previously thought. But there is no room for complacency, and security teams are burdened with an unenviable task of ensuring compliance while remaining accessible—and maybe even popular. To do this, it might help to look at various behavioral tools that can help.

And ultimately, that leads into a discipline that appears at odds with the highly-technical infosec world—marketing, and more specifically, internal marketing. The most effective internal marketing campaigns have typically started with a "shock." Sometimes, this is as grand as a wholesale rebranding, or a change in leadership. But sometimes, it can be as simple as the decision to change.

That was particularly true to IBM in the early 2000s, which was facing a period of business and technological stagnation, compounded by several embarrassing setbacks, such as the failure of its OS/2 operating system. The incoming CEO, Samuel J. Palisano, argued that any rebranding would be pointless without a cultural shift. This ultimately resulted in the creation of a set of three core values that have endured since.

For your IT security team, you can create your own "shock" by defining what you aspire to be and what you aspire to achieve. Create a blank slate, as it were.

Behavioral economics reinforces the need for that "shock," noting the existence of a cognitive bias called "status quo bias." This means that behavior tends to stay static unless there is a sufficiently strong reason to change it.

Consider the scenario where someone is driving a car on a wet day. While the voice of reason and road signs may implore safer driving, it's not until the back end slides out and there's a fleeting moment of fear that the driver adjusts their driving. The shock of nearly losing control can be a far more powerful trigger to change behavior.

Another useful cognitive bias—which also appears heavily in behavioral psychology—is the bandwagon effect. In short, people are more inclined to alter their behavior if they see other people acting in that way. And while this bias may be uncomfortable to acknowledge because it undermines the belief in our independence, it is nonetheless essential for security teams looking to improve compliance. It underlines the importance of having clearly defined policies and ensuring they're widely known.

Going back to a car analogy; children are far more likely to put on their seatbelts if they see their parents, other adults and siblings put on theirs before any journey. They may not fully understand the reasons why, but the bandwagon effect, especially when observing adults (or in a corporate scenario, leaders) adopt certain behaviors, they are more likely to follow suit.

Ultimately, any rebranding should be positive in nature. Psychology shows that people have a so-called negativity bias. In practice, this means that people are more likely to change their behavior to avoid unpleasant experiences. If your department has a reputation for being harsh with offenders or tying workers with red tape, there is a higher chance that your colleagues will merely try to avoid you entirely.

By marketing your team as a positive entity, free from judgment and admonishment, the odds are good that engagement will improve as a result.

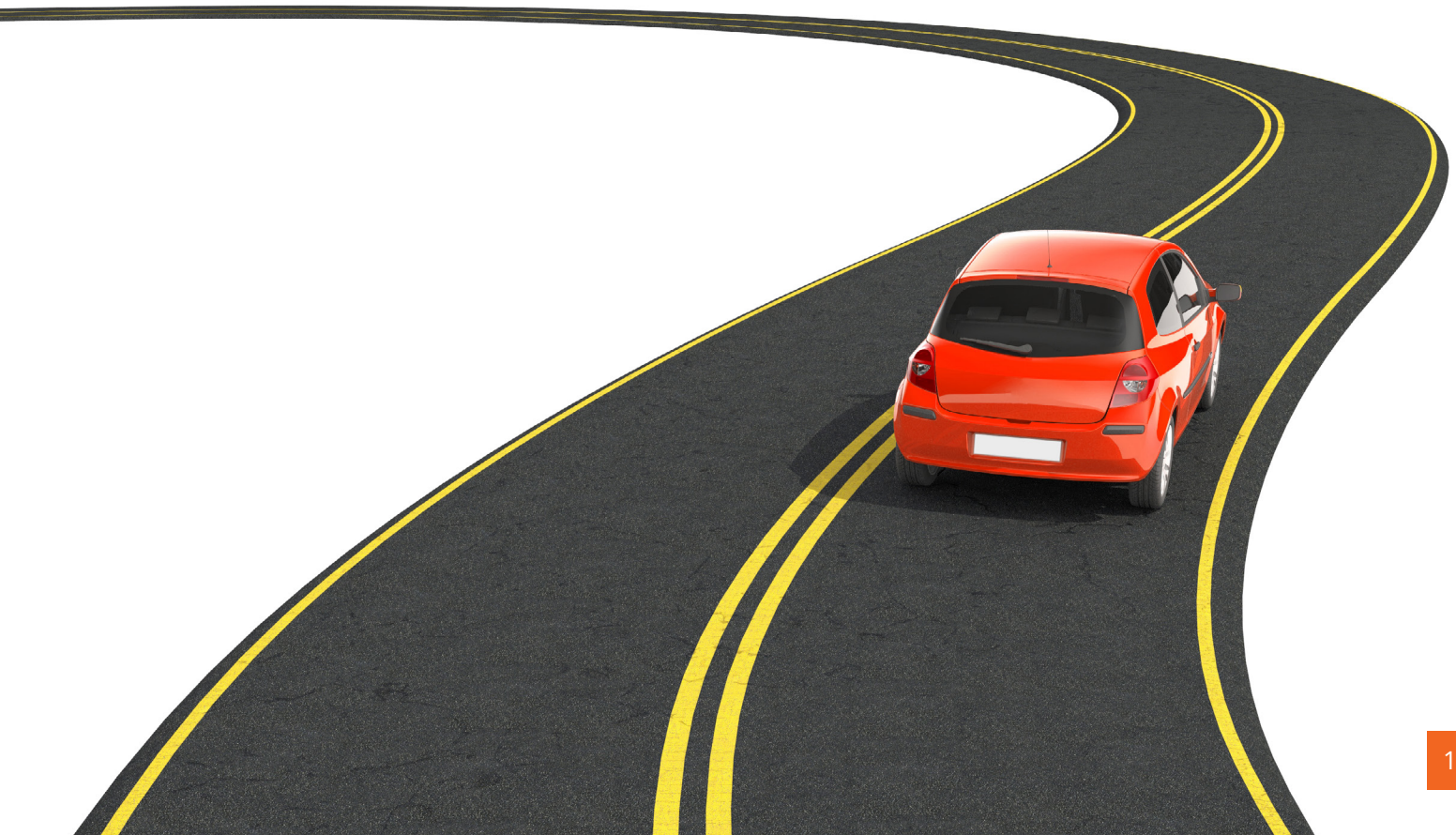
Conclusion

If you're reading this, chances are high that you're a technical person, or someone used to managing a team. You aren't a marketer. And yet, marketing is a skill that'll inevitably prove invaluable as you attempt to create and promote your newfound security brand.

Your journey should start with thinking about what you want your team to represent. Try to understand the pain points in your organisation. Don't be afraid of having a frank conversation about your previous shortcomings.

And then, resolve to fix them. Think about ways to make your department approachable. Office hours, like those used in Transferwise, are a great start. And don't be afraid to have a two-way conversation, giving feedback and kudos to those in other parts of the business.

Creating a positive feedback loop will have a cumulative effect, help wash away any previous bad impressions, and make others more likely to engage with the all-important security process.



Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customised Security Awareness Program for your organisation

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realising that the human element of security was being seriously neglected, KnowBe4 was created to help organisations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organisation with security top of mind.

Tens of thousands of organisations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilise their end users as a last line of defence and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com
KnowBe4 UK, Ltd. | Osprey and Kestrel, The Hawkhills Estate, Easingwold, York YO61 3FE | +44 (0) 1347 487512

V073020