TANIUM

IT Trends 2023

The Move to a Risky Cyber Stance?

Foreword

Cybersecurity is a high stakes game that requires cool minds to prevail in times of uncertainty. But as we look towards 2024, are IT and security leaders being given enough latitude to protect their organisations against emerging threats?

As part of a far-reaching study, Tanium asked a large sample of business and technology leaders for their views on how cyber is perceived today. Has there been a breakthrough of understanding in the boardroom? Or is the IT domain still on the outside looking in? Read on as we reveal all in our latest annual cybersecurity trends report.

Our research covers the ground that you don't often see in industry studies of this type. We've probed into the reasons why organizations' security stance may have changed – not just if it has or hasn't. We've quantified whether there is agreement or dissent in the IT ranks when it comes to organisational policy and attitudes to risk. Ultimately, we reveal whether the security domain is happy with the hand they've been dealt.

What does all that mean going forward? We've consulted with independent experts in the industry and even some of our own business leaders to add that all-important context. So, without further ado, let's delve into the findings.

A different flavour of cybersecurity

The big picture view is that a large number of organisations intend to change their security posture in next 12 months – becoming more reactive in their approach to cyber.

Although the majority (65%) currently operate with a prevention-first approach, 20% intend to switch stance in the year ahead. Should this occur, that would be the first time that most enterprises were, by default, reactive.

This is one of the more surprising outcomes of Tanium's annual cybersecurity survey of IT and business leaders in the UK and Europe. So, what's changed? Why the change of heart since last year when we ran a similar study?

The simple answer, as far as our survey sample is concerned, is that they're simply following orders. Half of the entire research base (51%) claim that they're responding to "board-level directives to focus more on reactive measures".

Not surprisingly, this isn't a course that IT professionals necessarily want to follow. 62% still think that "a preventative approach to cybersecurity is the best" considering that it costs more to fix a breach rather than prevent it in the first place.

> 55% went to say that their Chief Finance Officer (CFO) doesn't "understand the extent of the threats we face", posing the question of whether cybersecurity is appropriately represented in the boardroom.

Puzzlingly, 75% said they actually do have such a voice on the executive team and, yet, they are "more likely to get sign off for cyber security budget" when a breach has already occurred – not before (73%).

This all leads us to ask: is there a storm brewing between the front line officers and the boardroom generals? Are those running the business speaking the same language as those protecting it? Are the CISO's powers of persuasion on the decline?

Sector breakdown:

- Doubling down: **78% of telecoms firms have a preventative approach and intend to keep it that way in the year ahead**
- Most reactive: **40% of organizations responsible for 'national critical infrastructure' will swap prevention-first for reactive cybersecurity**

"There has been a small but noticeable shift away from prevention-first, which clearly goes against security professionals' best instincts. But this is a business-level directive that's simply a response to the current macro-economic conditions.

CFOs and their fellow executives know perfectly well the operating risks of switching approach. They simply asking the business – including IT – to tighten their belts and keep the lights on. It's for CISOs to convince them that precautionary cyber spend isn't discretionary and will provide a return. At the moment, their attitude is that they can't fund something that might never happen."

Zac Warren
Chief Security Advisor, EMEA, Tanium

The cracks are beginning to appear

If IT and security professions are being asked to focus on the here and now – and not just the preventable future – what does the threat landscape look like?

Overwhelmingly, the majority (72%) think that this year will be the worst year on record for cyber incidents by volume. This is up from 69% who made the same prediction in last year's survey.

So why the company-wide focus on more reactive security measures if the threats, attacks and breaches expected to continue? Surely more prevention is the cure? 47% cite the "lack of confidence in managing all our endpoints", while 44% highlight the "disconnect between IT security and IT operations". Slightly fewer note the "lack of budget for preventative measures and tools" (40%) as well as the lack of "staff resource to focus simultaneously on preventative and reactive" (34%).

> Most tellingly, 51% say their business is prioritises a reactionary approach due, specifically, to "board-level directives". This, despite the fact that new compliance regimes are set to come into force during 2024 and 2025 including NIS2 and DORA, respectively.

With significant concerns over the volume of attacks, the size of the IT estate and the people or tools to manage it, perhaps we should anticipate that cybersecurity funding may be on an upwards trajectory? Not so, it appears.

Two-thirds of our poll (66%) say that "securing budget for cybersecurity tools and resources is a challenge for us". To compound matters, the shift to a more reactionary approach doesn't come without consequences. Eight out of ten (82%) of those we surveyed say it "costs more to recover from a cyber incident than prevent one".

An identical number also state that "investing more in a preventative strategy would minimise the impact of avoidable incidents", such as phishing and devices left unpatched. And, for avoidance of doubt, most cyber pros (78%) believe that the majority of attacks they've experienced were avoidable.

Sector breakdown:

- Most vulnerable: **88% of energy and utilities companies say that cyberattacks they've experienced were "avoidable"**
- Board-level input: **83% of retailers have "appropriate" cybersecurity input on the executive teams. Infrastructure (60%), education (67%) and telecoms (67%) firms have the least**

"In light of the growing challenges that security pros are up against, it does seem that organizations are taking somewhat of a gamble. It begs the question of whether executives are aware of forthcoming regulations, like NIS2 and DORA, that will compel firms and their boards of directors to increase the security and resilience of critical infrastructure and essential services.

Failure to comply can have several adverse consequences for financial institutions on an operational and financial level, but also in terms of brand loyalty. Not only do they risk regulatory penalties, reputational damage and loss of business, but they also run an increased risk of operational disruption."

Zac Warren
Chief Security Advisor, EMEA, Tanium

The buck stops here?

Although our study reveals a shift towards a more reactive security posture, it's clearly one that businesses haven't taken lightly. There appear to be very real, practical reasons why prevention has taken a back seat (for some). The biggest of those appears to be the limitations of existing, in-house teams. Both perceived and actual.

67% of our research sample say that their organisation "does not have enough staff" to focus on preventative measures. Does this suggest that IT teams are under-resourced, under-funded or under-skilled?

Well, all three could be legitimate concerns but what we know is that 76% find it "easier to secure additional budget" when they are "outsourcing to a partner". This points to firms' growing desire to forgo capital costs (including staff wages) in favour of operational expenses (including third party fees, licenses and subscriptions).

Employee awareness features right at the top of the chopping block with more than a third (36%) cutting back here. But there are other areas of security that are subject to internal austerity too. Remote workforce infrastructure (35%), new endpoint devices (32%) and data recovery/backup (30%) have all been trimmed down. The risks of making these changes are not lost on our cohort of IT professionals. They feel it personally. More than half (56%) lament the fact they are "being held personally accountable" but "not given the tools or budget to do the job".

70% go on to say that they have "concerns" about being held "personally accountable" for a cybersecurity breach – with three in four (75%) believing that the "c-suite should be held accountable" instead. Pretty damning stuff and a clear sign that the debate about personal versus organisational accountability is far from over.

Whatever differences of opinion that may or may not exist, most of our survey sample are confident they've identified the causes of their cyber issues. 69% say they have "clear understanding of where the gaps are".

63% would attribute this to shortcomings in their cybersecurity technology. The common complaint being that is only gives insights to "a portion of our data". A similar number (55%) say they "don't have visibility of all our endpoints" and are "unsatisfied" with their "current cybersecurity solutions" (52%).

Sector breakdown:

- Corporate accountability: **83% in banking and finance say that breaches are ultimately the responsibility of the organisation**
- Least satisfied: **IT stakehkolders in the education sector (61%) are least happy with their cyber tech solutions, followed by those in health and social care (56%)**

"President Truman was famous for having a sign that read 'The Buck Stops Here' in his Oval Office. IT teams want the reassurance that their business leaders feel the same way about cybersecurity issues. They want to know that it's not all on their heads. They want to know they're not being short-changed by their own organisation.

There's a certain resentment at play here and general feeling of being underfunded and underappreciated. But we should remember that board-level executives already have their hands held to the fire compliance-wise. That's only going to persist with new regs coming through. Regs with actual teeth. The IT and security function could help its own cause by getting ahead of this and communicating why it's good for everybody to be invested and fully prepared now – not when an incident occurs."

Zac Warren
Chief Security Advisor, EMEA, Tanium

Final thoughts

What are the big takeaways from this year's cybersecurity trends report? Firstly, we should acknowledge that the appetite for preventative cybersecurity has dimmed. But that's not the same thing as saying most boards no longer believe in it. Even from a self-preservation point of view, most executives know they need more protection – not less.

However, it's clear that cybersecurity funding has come under greater scrutiny – becoming more aligned to way other business units experience it – with ups and downs.

The good news for cybersecurity and ITOps professionals is that more regulatory oversight is imminent and that's an opportunity to reverse the trend and win back share of wallet internally.

The question is how they secure it and what they then do with it. By their own admission, security pros are dissatisfied with their current tools and limited visibility of assets across the IT estate. This is the obvious starting point to tackle the belief that they are being held accountable for things they can't control.

If the business-wide problem is visibility (and it certainly appears so) then IT, operations, security, and risk and compliance teams all need to focus on that central objective. Company boards want visibility too, but they won't pay for each department to have their own particular brand of it. They want a single source of truth and a real-time understanding of the threats facing the business.

What everyone wants to avoid is accountability without visibility.

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the Power of Certainty™.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

© Tanium 2023