HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security   **PUBLIC/ UN-SPONSORED**

HardenStance's RSAC Survey Report

Here's what HardenStance's survey of industry leaders conducted during RSAC 2022 in San Francisco last week tells us about the state of cyber security in June 2022:

▪ Asked what single factor can drive the biggest improvement in cyber security, leaders in the vendor community have a variety of priorities. Consolidating from those disparate responses they prioritize education, authentication and operations.

▪ The most common belief is that the single most important thing we can do to improve our resilience is drive better cyber security awareness, education and training. The second priority is more efficient, more effective, security operations. The third is greater adoption of Multi Factor Authentication (MFA) and Single Sign On (SSO).

▪ Only 25% of respondents pointed to any kind of point product as priority number one – and most of these pointed to MFA & SSO which those respondents' own companies don't themselves sell.

Survey Methodology

During RSAC 2022 last week, HardenStance met with 24 leaders from leading cyber security vendors. These were all Director, VP or C-Level Executives representing a variety of different companies (see **Figure 2** on page 5). HardenStance concluded these meetings with a single, open, question for the meeting host.

The question was entirely open – respondents answered freestyle with whatever popped into their heads.

Respondents were not given a menu of response options or asked to tick a box. The question was entirely open – they answered freestyle with whatever popped into their heads. Before being told the question, individual respondents were asked to consider their answer for 20 seconds before answering. They were also told that their answer would be anonymized (and that the answer couldn't be 'buy my product'!)

The question asked was:

"What is the single most important thing we can do – whether drawing from the world of business, education, politics, technology, finance, or any other – to improve the security of our digital infrastructure and improve cyber security outcomes?"

The full survey results and supporting data follow on the next page.

Results of the HardenStance Survey

The break down in survey responses is shown in **Figure 1** below. The individual anonymized statements are shown on pages 3 and 4. The first take-way is just how diverse the thinking is about what buys us the most 'bang for our buck' when it comes to cyber security. The 24 responses generated 14 completely different types of answer.

The high level takeaway is that what buys us the most bang for our buck in cyber security is improvements in education, authentication and operations. The answer given most often was better awareness, education and training, called out by 25% of respondents. These answers pointed to the need to upskill the knowledge of all users ranging from consumers to IT administrators to infosec professionals themselves.
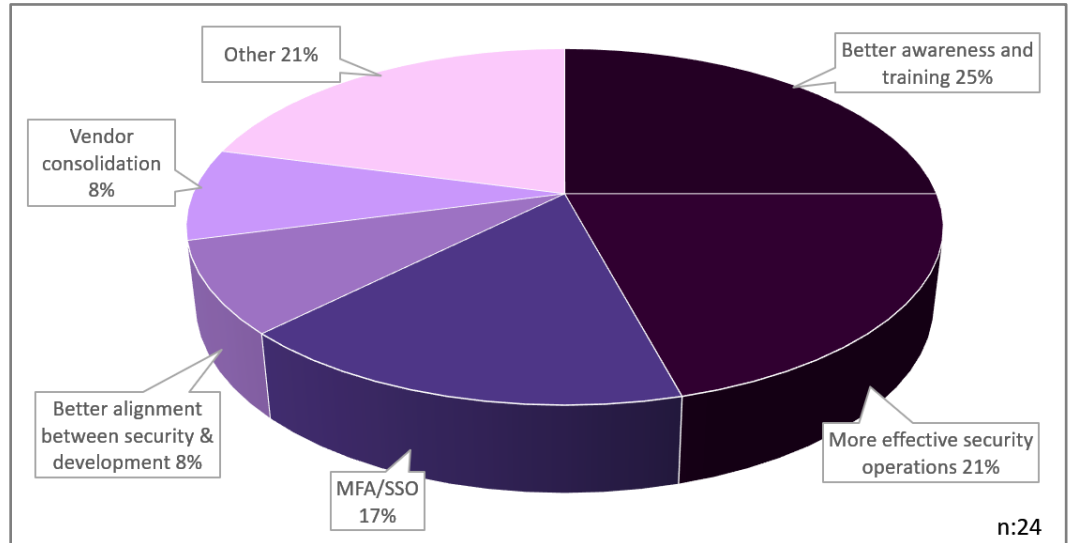
More efficient, effective security operations

The second most popular response was more efficient, effective operations, cited by 21% of respondents. To be clear, not one of these individual respondents even used the word "operations" in their answer. However, for the purposes of this survey, all of these responses – respectively citing continuous risk assessment; visibility; easier management of migrations; stronger collaboration and accelerating automation – can legitimately be grouped under a broader security operations theme.

In third spot, with 17% of responses, cyber security leaders pointed to Multi Factor Authentication (MFA) and Single Sign On (SSO). The only other categories to generate more than one mention was vendor consolidation and better alignment between security and development teams – each one nominated by two respondents.

New technology barely featured at all among responses. Only 25% of respondents pointed to any kind of point product as priority number one – and most of those nominated MFA & SSO which those respondents' own companies don't even sell. This serves as a useful reminder that while vendor leaders determined to get an ROI out of RSA are certainly predisposed to 'sell, sell, sell' their own product, they are also able to switch gears when asked to and point to fundamental priorities that their own, often more advanced, product lines don't directly serve. For that same reason, 'AI' and 'ML' didn't garner a single mention by anyone – when the focus is on what's to be gained from fixing some of the basics, the advanced stuff isn't top of mind.

The answer given most often was better awareness, education and training, called out by 25% of respondents.

Figure 1: The Single Most Important Thing That Would Improve Cyber Security

Source: HardenStance

As you might expect, CEOs proved more likely to point to bigger picture finance and political issues. One pointed to the need for a substantial market correction to curtail the power of the VCs in driving "insane" behaviour by other security vendor CEOs. Another pointed to the need for "stronger retaliatory action" to punish cyber threat actors. ∎

"What They Said" – Here's how the 24 Respondents Answered

What Drives Most Progress? Education/Training (25% of answers)

"Better education and training – of consumers and IT and IT security teams"
Director, Product Marketing, Information Management Solutions Vendor

"Training – there are too few people to manage all these sophisticated tools. We either need more people or less sophisticated tools "
Founder, Threat Intelligence Solutions Vendor

"Awareness and training – people are too easy to cheat."
Head of Security Services, Network Vendor

"The biggest factor is human error – we have to get better at training people so that they don't do things like clicking on a bad link."
Director of Product Marketing, XDR Vendor

"Better education and awareness on the part of security solution users and buyers"
Director, Product Management, Network Security Vendor

"A better understanding of what it is we most need to protect"
Director, Product Marketing, Network Security Vendor

What Drives Most Progress? Effective Operations (21% of answers)

"Continuous Risk Assessment – rather than 'one and done' "
Director, Product Marketing, Telco MSSP

"Visibility – you can't protect what you can't see, what you don't understand."
Director, Product Marketing, XDR Vendor

"Easier, more flexible ways to manage migrations"
VP, Security, Networking Vendor

"Better, stronger collaboration. There's so much data, it's changing all the time. No one enterprise SOC team has enough resource to do this themselves."
CTO, Network Security Vendor

"Accelerate the rate of security automation and eliminate humans – humans screw up."
Senior VP, Global Software Development Outsourcer

See the other responses on the next page

What Drives Most Progress? Authentication (MFA/SSO) (17% of answers)

"SSO, 2FA, lose Microsoft Exchange and shift to O365. Stop trying to do everything yourself."
CTO, Cyber Ratings Vendor

"MFA for consumers, as Google has shown. SSO shouldn't be such
a steep premium in the business market either"
VP, Product Marketing, Cyber Asset Management Vendor

"Enforce Multi Factor Authentication"
VP, Innovation, Home Network Security Vendor

"Back to basics: 2FA, MFA, do your patching"
CEO, Cyber Ratings Vendor

What Drives Most Progress? Others/outliers (37% of answers)

"Security teams need to hire more developers. Security isn't just about configuring devices any more.
You need developers implementing solutions via APIs. Web Application Firewalls (WAFs) available as
Microsoft tools, that's the way this is headed now."
VP, Product Management, Network Security Vendor.

"We need more empathy across security and development teams. The ways in which they don't take
account of one another's needs creates a lot of problems currently. We need more security people
that have been developers and vice versa to address that."
CTO, Zero Trust Vendor

"Vendor consolidation – there are far too many vendors".
VP, Product Management, Telco MSSP

"Vendor consolidation – there are too many vendors".
VP, Public Affairs, Ethical Hacking platform

"Really good protection technologies"
VP, Marketing, XDR Vendor

"Do a better job of protecting Active Directory using now widely available automation tools.
It's where the attackers go. It's where the Red Teamers all go. Deny them access to
that and there's not a whole lot more they can do.
CMO, Endpoint Security Vendor

"The VC model driving a lot of cyber security vendors is insane. What's needed, and what I see
starting to happen, is a major financial correction which the market will take care of."
CEO, SASE-like start up.

"How about we just build a better Internet?"
VP, Product Marketing, Cyber Security Posture Management Vendor

"Stronger retaliatory responses. At the moment these bad actors are doing all this stuff
and they're not suffering any consequences"
CEO, Network Security Vendor

Figure 2: Job Titles of the 24 Survey Respondents

Job titles of the 24 Director, VP & C-Level cyber security leaders making up the survey sample	
CEO, SASE-like start-up	Director of Product Marketing, XDR vendor
CTO, Zero Trust vendor	Director, Product Management, Network Security vendor
SVP, Global SW development outsourcer	VP Product Management, Telco MSSP
VP, Public Affairs, Ethical Hacking Platform	VP Marketing, Security Posture Management vendor
VP, Innovation, Home Network Security Vendor	CEO, Cybersecurity Ratings vendor
CTO, Cybersecurity Ratings vendor	Director, Product Marketing, Telco MSSP
VP, Security, Networking Vendor	Director, Product Marketing, Network Security Vendor
CMO, XDR Vendor	VP, Product Management, Network Security Vendor
Head of Security Services, Networking Vendor	VP Product Marketing, XDR Vendor
Director of Product Marketing, XDR Vendor	CEO, Network Security vendor
CTO, Network Security Vendor	Founder, Threat Intelligence Solutions Vendor
Director, Information Management Vendor	VP, Product Marketing, Cyber Asset Management Vendor

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum.

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.