FIRMWARE SECURITY

in financial services supply chains

Ramy Houssaini
Global Cyber Resilience Executive

Faster than the other guy

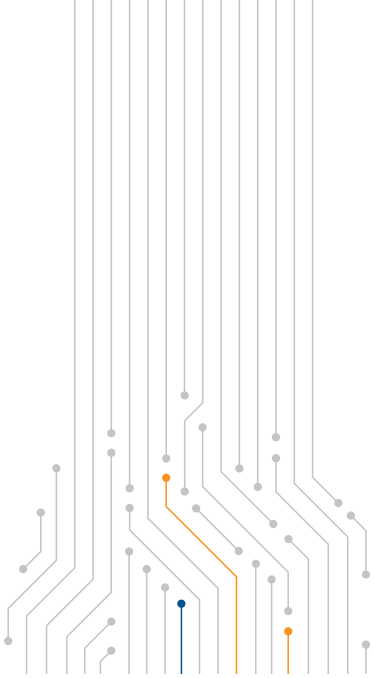
There's an often-told joke in cybersecurity that starts with two people running for their lives from a bear. Who can run faster than a hungry bear? The punch line, of course, reveals survival doesn't actually depend on both people being able to run faster than the bear. Survival is assured if one person can just be faster than the other.

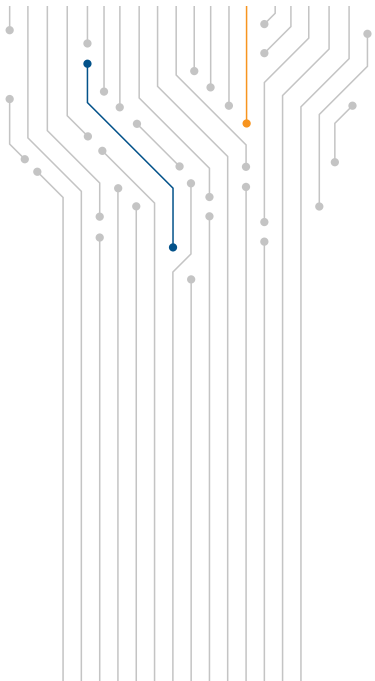
Like all jokes, we laugh because at its most fundamental level, this story feels true. There's a surfeit of targets and adversaries out there, from nation state sponsored to criminal threat groups. This surplus makes it easy to harbor the secret belief that if we're just "faster than the other person" – with better defenses or better threat detection or faster reaction times – we can avoid being the next breach headline.

The reality, of course, is that in every one of our networks and in every organization we have both profiles of runners represented: we have critical systems that are protected and patched and well-provisioned and staffed and they run like Usain Bolt. We also have systems and segments (and sometimes whole supply chain ecosystems) that are really mostly ignored, vulnerable and overlooked targets. Firmware – the embedded critical code present in every piece of hardware – is often like this.

Firmware tells every element of our technology supply chains – from hardware components and chips to entire devices and infrastructure – how to operate and what to do. It's the most privileged and powerful code to run in any system. It's critical to end-user devices, servers and network devices, and threat actors love it. They love it because compromising firmware compromises the entire software stack and all data inside devices, securing which is a critical pillar of zero trust architecture. They love it because they've learned how to infect it such that our security controls are blind. Firmware has taken "The Other Person" crown by being the slowest moving target in our technology supply chains.

This survey reveals how much cyber risk decision makers in financial services companies know or rather don't know about the state of firmware security in their device fleet and supply chains. It shows how much more they need to prepare for device-level and supply chain attacks. It also reveals how the false distinction of "me or the other person" has fully disappeared. We all rely on devices with millions of lines of critical device-level firmware code and extremely complex network of suppliers that develop it, and in almost every case it is the weakest link in our race against attackers. It is about time for us to collectively change this dynamic, recognize our exposure and address it.





Introduction

The world has changed remarkably in the last few years. We are assured it will continue to do so, particularly for those in enterprise-sized financial service organizations who are often the first to feel the ripple effects of global changes. There are constant expectations to serve customers at the highest level, while using the most innovative and advanced technologies throughout increasingly complex global supply chains. For the most part, this is a good thing.

However, organizations must be able to secure these technologies, both new and old. Cyber threats are becoming more advanced with every passing day and cyber criminals look for new ways to gain leverage. They act with a degree of speed and agility that often leaves target organizations trailing. So, in response, one would expect IT security departments to cover all existing bases. Wouldn't one?

Worryingly, this is more often than not, not the case. As we investigate through the course of this report, most organizations are still struggling with what should be a basic requirement: securing the embedded firmware their devices and supply chains rely upon. Whether we ascribe this lack of knowledge to lacking the proper tools and training, being chronically overworked, or simply negligent, we find that organizations are leaving themselves at the height of vulnerability. For too long this has been an open path for cyber criminals to cause chaos among organizations, but it is time for that to change.

This whitepaper, informed by interviews with IT decision makers with knowledge/responsibility for IT security (IT security DMs) in the financial services sector and a comprehensive three-continent survey, looks to explore several areas including, but not limited to, the following:

- Current awareness and understanding of firmware
- Financial investments in firmware protection
- Firmware attack experience
- Confidence in ability to respond to a firmware-level attack

Key Findings

76% of IT security decisions makers (DMs) in the finance industry have gaps in their awareness concerning their organization's firmware blind spot

91% are concerned about the gap in firmware security in their organization's digital supply chains

92% admit that cyber criminals are better equipped to attack firmware than their organization is at protecting it

88% are aware that their organization has been the victim of a firmware-level attack in the last two years

93% of IT security DMs are surprised by the lack of insight into current firmware threats

Section 1: Current awareness and understanding of firmware

You'd be easily forgiven for thinking that IT security DMs have complete control and knowledge over all things cybersecurity related. But, this isn't the case. There are often gaps in teams' knowledge, whether that be through a lack of skill or qualifications, a lack of human resource, or a lack of investment.

This gap in knowledge becomes quickly apparent during our review of survey data from IT security DMs' responses. Fewer than half were aware that BIOS (Basic Input/Output System) (45%) or UEFI (Unified Extensible Firmware Interface) (44%) are examples of firmware. Even fewer believe that Intel ME (Intel Management Engine) (41%) or BMC (Baseboard Management Controllers) (37%) are examples of firmware. These are, of course, not only perfect examples of embedded, vendor-supplied firmware, but also excellent examples of active, targeted and successful exploits by our adversaries (see these links for UEFI examples or for BMC examples).

On a similar note, there is a distinct lack of knowledge around the types of devices that rely on firmware. Only 53% believe that their security controls rely on it, with fewer than half who say the same about network devices (47%), laptops (44%) and computer peripherals (41%). It's only around one in five who have this awareness regarding optical drives (21%) and headphones/headsets (19%).

This should be a significant red flag for organizational security awareness. Each of these device types rely heavily on a complex supply chain and the firmware injected into it at various points, and this gap in awareness will lead to a gap in security. Ultimately it will leave costly thorns in these organizations' defenses.

Awareness of devices that rely on firmware

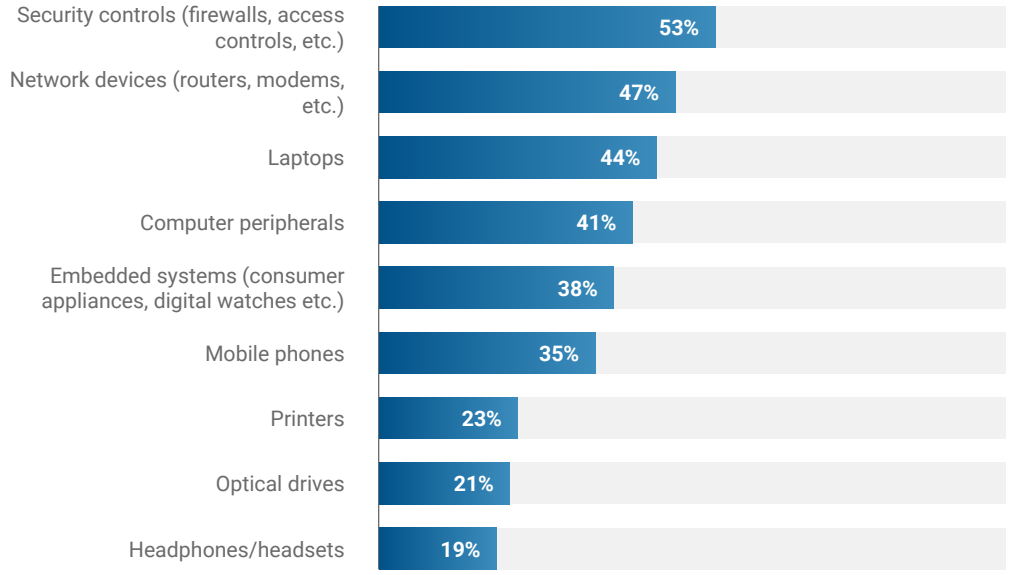


Figure 1: Which of the following device types do you believe rely on firmware? [350], omitting some answer options

After these initial questions, we provided respondents with a definition as to what firmware should be considered as (see below). When adding this context to the following data, it corroborates the early indication that considerable gaps exist in current knowledge levels. It also highlights where these gaps are.

"Throughout the rest of this survey, please consider firmware to be a type of software or code that is etched directly into a unique hardware component. It usually operates without going through APIs, the operating system, or device drivers—providing the needed instructions and guidance for the device to communicate with other devices or perform a set of basic tasks and functions as intended. Firmware is inserted throughout an entire supply chain, and on a range of devices that includes laptops, peripherals, network devices and printers."

This lack of knowledge becomes even more troubling when we consider the perceived awareness that our respondents have. Almost half (47%) feel they have total awareness of their organization's overall firmware attack surface, while a similar proportion (49%) report being mostly aware. There's a sense of déjà vu when considering that 23% of respondents feel that they are totally aware of their organization's firmware blind spot, with 58% who say that they are mostly aware and only have small gaps in awareness; we know that respondents are unlikely to be as aware as they feel they are given the missing knowledge on what firmware is, the devices that contain firmware, and the supply chain's reliance on it. This overconfidence is almost as dangerous as a gap in knowledge and security itself.

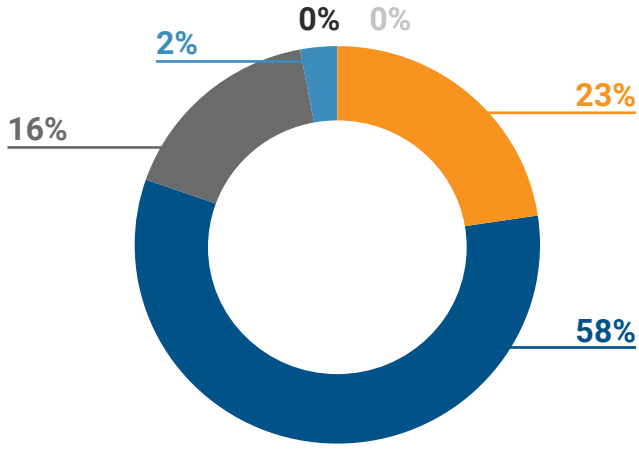


Figure 2: Traditional security tools do not operate "below the OS" where firmware lives. Are you aware of the scope and size of your organization's "firmware blind spot"? [350], omitting some answer options

If there is one silver lining, IT security decision makers do seem to have an awareness of the issue, with a large majority (91%) feeling concerned about the gap in firmware security. This should leave an appetite to improve and further tighten the security of firmware and the supply chains that convey it. Unfortunately, this isn't always the case.

Section 2: Financial investment in firmware protection

With this data we have an understanding that perhaps ITDMs and their organizations are unlikely to be as well-equipped and knowledgeable as they could be when it comes to firmware. But where does that leave us with investment and strategic priorities?

Firstly, taking a broad view, the global spend for the information security and risk management market stands at $172.5 billion (current U.S. dollars) in 2022 and will reach $267.3 billion by 2026, according to data from research firm Gartner. On average, each organization spends almost $14 million apiece on IT security. On the surface, this seems like a very significant investment. However, when you consider how broadly this needs to be distributed to implement and maintain a range of security systems and protect against a variety of threats, it will run thin very quickly.

That spreading of budget is only too apparent when we look at the proportion that is dedicated specifically to firmware security. It is only around 4.5% on average which is earmarked for this specific outlay. This may seem like a reasonable proportion for one element of IT security, but when we go on to look at the potential threats in section three, it becomes clear that this may well come far short.

Promisingly, this could be set to rise in the future. ITDMs anticipate that the proportion of IT security budget dedicated to firmware will rise by around 8.5% in the next 1-2 years. This indicates that organizations are starting to understand there is a shortfall in budget allocation, at the same time the threat of firmware-level attacks becomes even more prominent or dangerous in the near future.

But is this expected increase sufficient? Perhaps not. More than six in ten (62%) respondents feel that firmware security should be invested in as its own dedicated tool, which with the current budget levels, seems unlikely to be feasible. There are almost four in ten (37%) who consider a dedicated tool and a shared tool to be appropriate, depending on the circumstances. Ultimately, if there is to be an investment into a dedicated tool of any description, organizations will need to put the investment into practice, otherwise they'll be left short and with a sub-par solution that doesn't provide the enterprise-wide assurance it needs to.

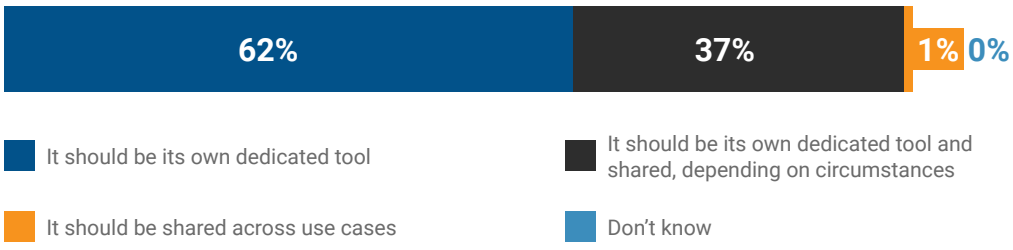


Figure 3: In general, do you think firmware security should be invested in as its own dedicated tool, or should firmware security use cases be shared (e.g. across VM, endpoint, infrastructure security tools)? [350]

Section 3: Firmware attack experience

It's common knowledge that IT security is critical to financial organizations, but many are yet to fully appreciate the new demands being made. Cyber threats are growing and organizations need to respond; as we have already seen, dedicated tools are becoming a necessity.

This becomes even more apparent when considering the devices that could be compromised by a firmware-level attack. Around half feel that network devices (54%) or laptops (46%) are most likely to be compromised; there are ample numbers of these devices within organizations, meaning that the potential attack surface is huge. With this in mind, it's easy to explain how **88% of organizations have been the victim of a firmware-level cyber attack in the last two years**. It's even more concerning when you consider that 55% have been the victim of this type of attack more than once – organizations are either not learning from their mistakes, or simply don't have the automated tooling and third-party expertise to prevent these exploits.

Victim of firmware-level cyber attack

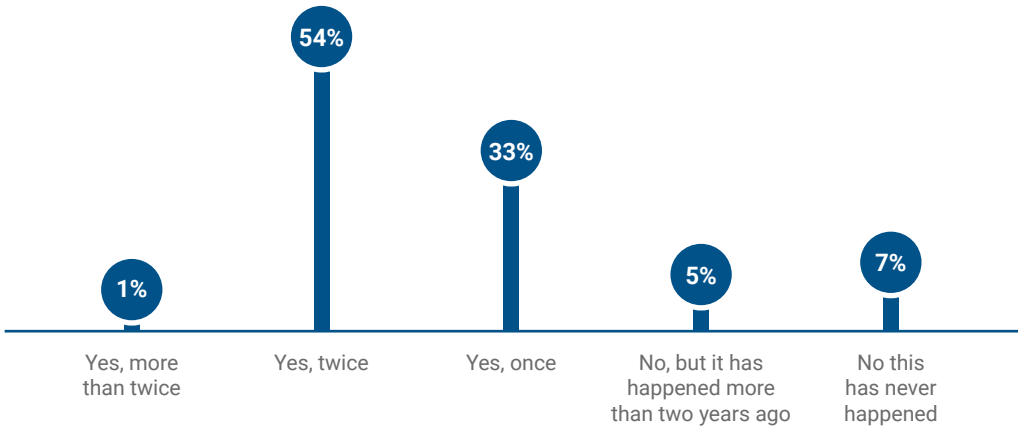


Figure 4: Has your organization been the victim of a firmware-level cyber attack in the last two years? [350], omitting some answer options

It's clear that firmware related attacks will result in organizations suffering, with almost all (99%) respondents reporting that there would be an impact if their organization was to fall victim of this attack type. Much like any other form of cyber attack, firmware related attacks can have incredibly severe consequences for organizations. Almost four in ten say that this would be a loss of data (and a GDPR breach) (38%). Many understand how reliant their security controls are on firmware, with a similar percentage (38%) who believe that a firmware-level attack could leave security controls ineffective. Furthermore, only a third understand, correctly, that firmware attacks could result in the destruction of critical devices (35%). Each of these impacts are likely to have an effect on the organization's entire supply chain and their bottom line, which then begs the question, why not invest more in securing firmware and avoid the damage?

Impact of suffering a firmware-related attack

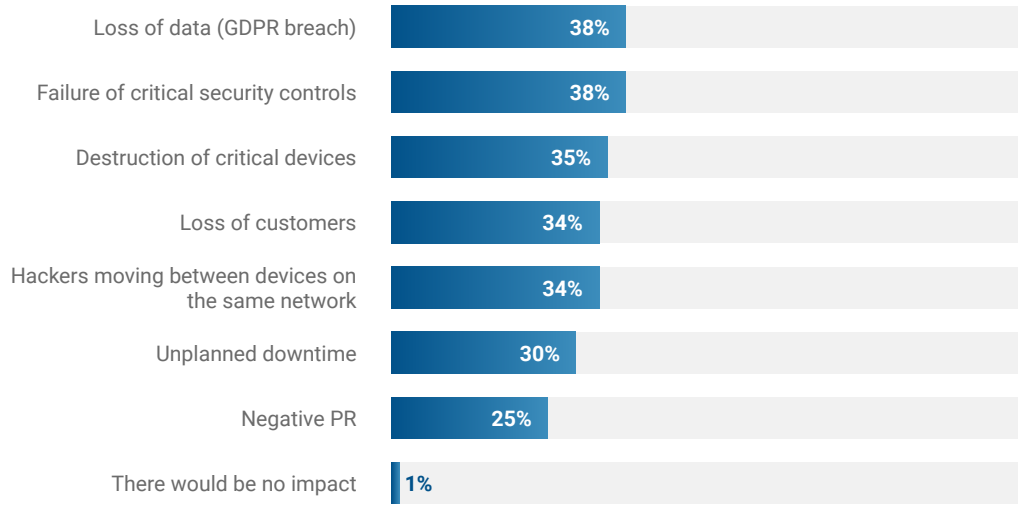


Figure 5: What would be the impact if your organization suffered a firmware related attack? [350], omitting some answer options

Perhaps the root of this under-investment is a misguided belief that existing security controls will absorb the brunt of firmware-related attacks. As a recent Security Boulevard article stated: *"Unfortunately, firmware attacks are challenging to detect, as they are often imperceptible and deeply embedded".* Despite this mis-perception a surprising number of organizations (81%) think their vulnerability management solutions can identify firmware vulnerabilities and assist in remediation processes. The objective fact is that most vulnerability management solutions can only assess the most common BIOS and UEFI firmware elements – perhaps a tenth of any system's critical firmware – and in most cases will simply parrot back what the operating system "believes" to be the state of firmware, which has shown to be highly spoofable. Networked and connected devices, which account for a high percentage of ransomware targets, run almost exclusively on firmware and are rarely covered by vulnerability management solutions.

A very similar proportion (83%) report that their endpoint detection and response (EDR) program includes detection and remediation for firmware-level attacks. Similar to the challenges with vulnerability management systems, EDR solutions can at best track one or two superficial firmware components. But more recent research by Gartner has revealed that every laptop and desktop computer ships with some 15-20 firmware components and that servers come with 30 or more components installed. Given these very realistic numbers, the firmware observability rate for EDR solutions is a dismal 10% to 13%. So, we come back to the same problem; organizations feel like they have solutions and processes in place, though they have a weak or uninformed

This narrative develops further when we consider that 94% of those surveyed believe threat modeling exercises should include firmware-level attacks that may render critical devices inoperable or unbootable. Almost four in ten (37%) say that this should always be the case. On the other hand, there's no point in that inclusion if the exercises are not relevant and this often seems to be the case. Over nine in ten (93%) feel that current threat modeling exercises are not relevant to modern firmware attacks at a device level. This indicates that firmware-level threat modeling exercises can or should be useful, but they need to undergo a massive overhaul – in technological capabilities as well as user education – to ensure relevancy against modern exploits.

Firmware-level attack practices within threat modelling exercises

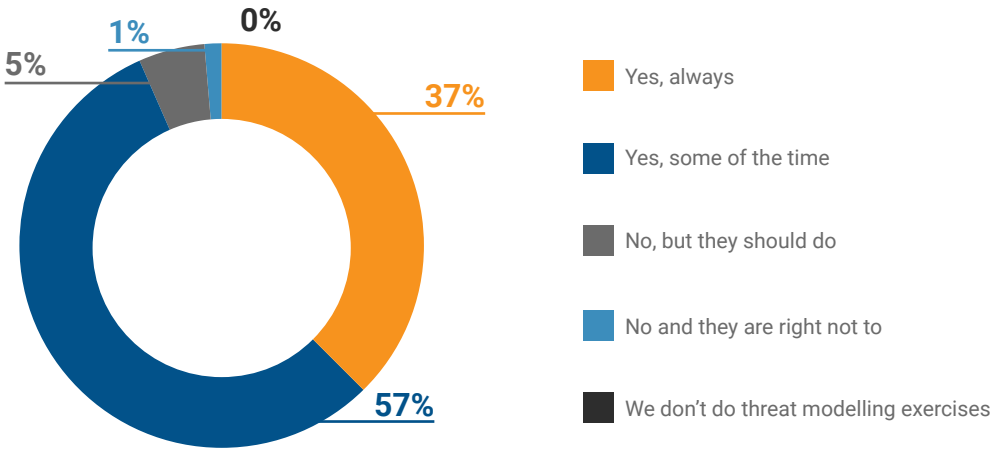


Figure 6: Do your organization's threat modeling exercises include firmware-level attacks that may render critical devices inoperable or unbootable? [350], omitting some answer options

The sentiment surrounding the improvement needed is optimized by the 96% who report that their organization's threat modeling exercises needs improvement as a whole. More specifically, a similar proportion (97%) state that the relevancy of their threat modeling exercises needs to be improved to better match today's threat landscape. Threat modeling exercises should be a vital tool in the IT department's armory, but it needs to be used correctly. These data suggest organizations must improve their threat modeling exercises to use firmware-based indicators of compromise. If they don't, they're likely to waste time and resources on irrelevant exercises and gain very minimal or no benefit from doing so.

Improvement required to threat modeling exercises

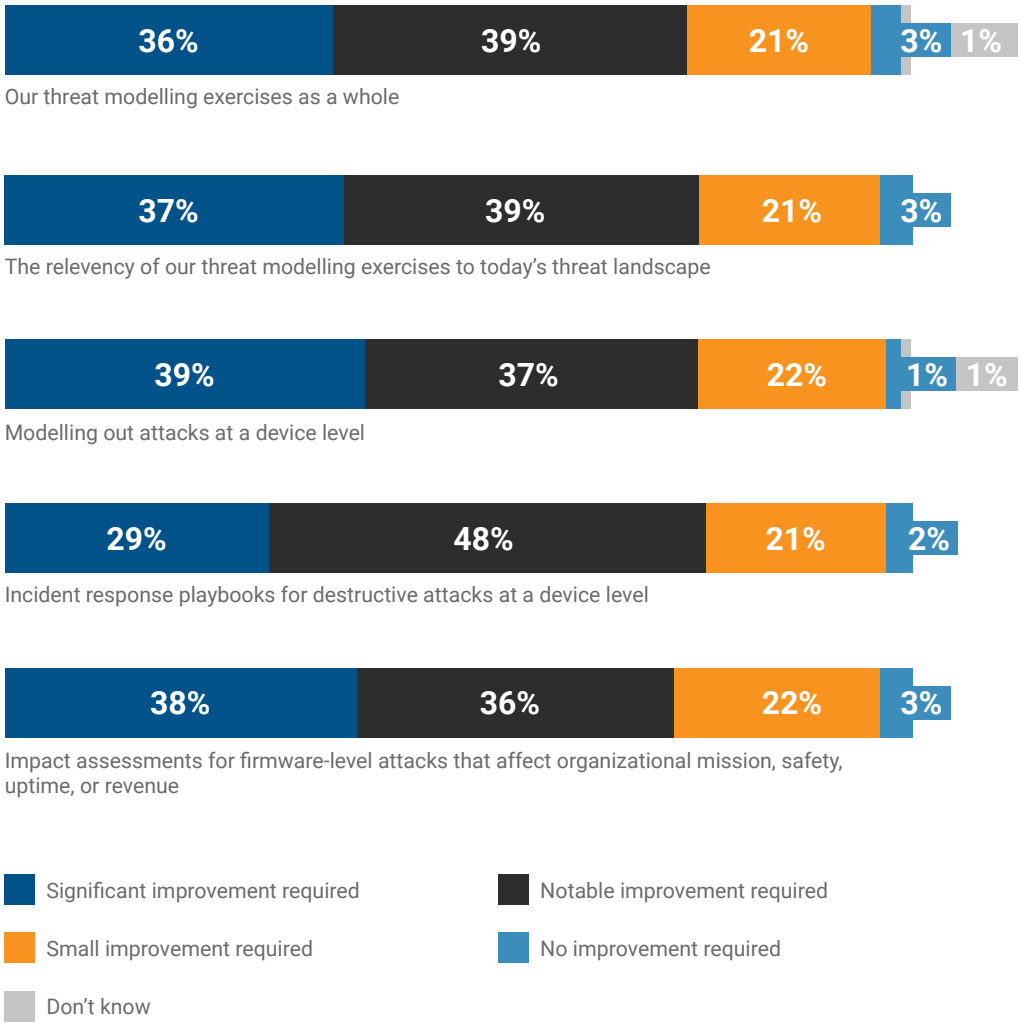


Figure 7: What level of improvement do you believe is required when it comes to the following aspects of your organization's threat modeling exercises? [349], asked to respondents whose organizations do threat modelling exercises

Section 4: Confidence in responding to a firmware attack

The need to respond to any form of cyber attack is of the utmost importance when protecting your organization and its data. But because organizations need to prioritize for the most damaging attacks, preventing firmware-based attacks that can "brick" critical equipment – wherever it exists in the end-to-end supply chain – rise to the top. This is particularly pertinent in light of the common misunderstanding of which devices contain firmware, and the consequence that exploit and breach detection will take far longer than it should. On average, respondents feel their IT/IT security team could respond to a firmware-based attack in 12 hours. That's plenty of time for a cyber criminal to move between devices on the network and cause havoc. In addition, it doesn't take into account any detection time, which may mean that the detection itself takes 6-12-24 hours, or more.

Response time is impacted by a number of events, regardless of the type of cyber attack. When reviewing firmware-based attacks specifically, it is most likely (39%) to come down to the same challenge, a lack of knowledge. This is another clear indicator that organizations need support in this area. On a similar note, 37% feel that a lack of human resource is hindering response time. In fact, it is only 3% who feel that nothing would hinder their response time.

Factors hindering response time to firmware attacks

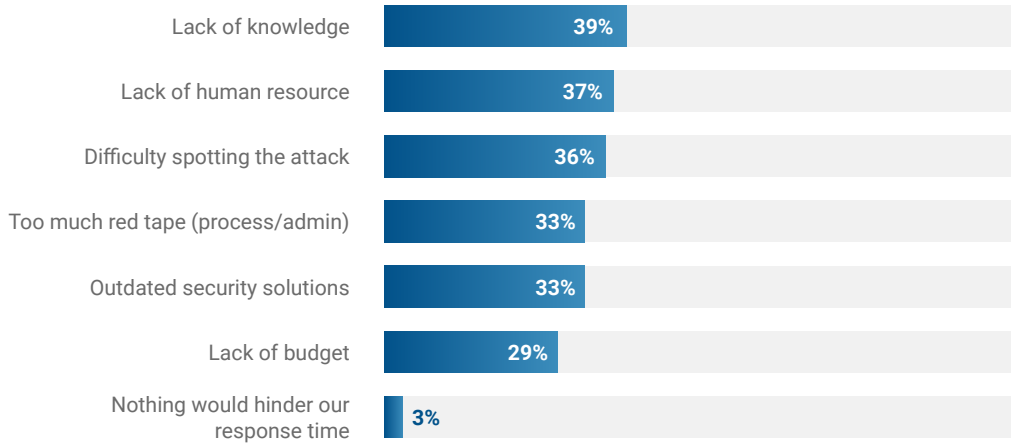


Figure 8: What factor(s) would hinder your organization's response time to a firmware-based attack? [350], omitting some answer options

When it comes to detecting a threat in the first place, it's clear that adversaries are becoming faster, smarter and more cunning. They are able to avoid detection better than ever before, and perhaps most alarmingly, they are able to seamlessly move around devices on a network undetected. Even if you catch them on one device, they could still be lurking elsewhere.

Bearing this in mind, it's surprising that 39% say that they would definitely be "immediately aware" if a device had been compromised at a firmware level and a hacker was living on it. This flies in the face of evidence from the wild that a firmware implant could "persist on the system even if the hard disk had been formatted or replaced." A further 60% say that they would probably be immediately aware. This sentiment is made clearer when we consider that almost all (95%) are totally or mostly confident that their organization's IT security team could detect firmware-level threats and hunt for firmware-based IOCs (indicators of compromise). This level of over-confidence in the ability to detect these nearly invisible attacks seems misplaced and creates an even bigger danger.

Immediate detection of compromised devices at firmware level

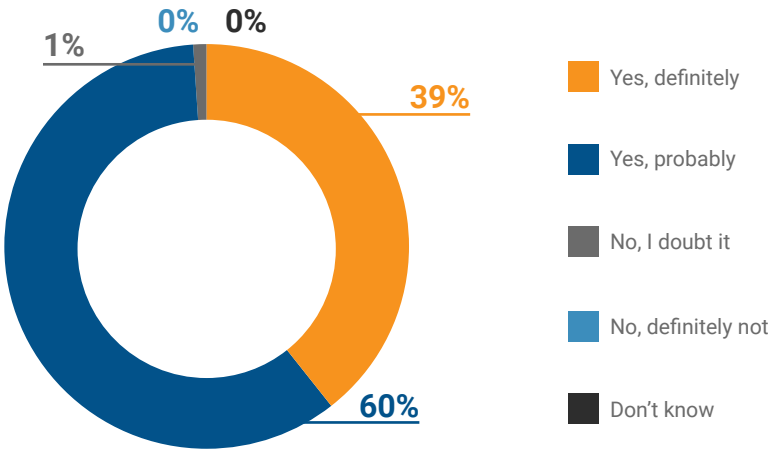


Figure 9: Would your organization be immediately aware if a device had been compromised at the firmware level and a hacker was "living" on it? [350]

However, it's clear organizations recognize they need change in order to fully protect firmware in their enterprise supply chains. **A strong majority (93%) of respondents say that an increase in financial investment is required, while a similar proportion (89%) feel human resource allocation needs to increase**. Organizations need to start making progress upon these changes. The threat towards firmware appears to be ever-rising; over four in five (83%) respondents consider vulnerabilities in firmware to be increasing. With change required and vulnerability growing, this should be a huge wake up call.

Given the intersection of an increasing number of firmware-based attacks, their lethality, and their impressive stealth, it's no surprise 93% of respondents state that securing firmware should be an urgent priority. Even if the right knowledge and infrastructure isn't in place currently, this is evidence of a strong desire for – and even movement towards – real change. Organizations seem to realize the threat is real and they must rapidly learn how to secure the vast, old, and largely unprotected attack surface represented by firmware in devices and supply chains.

Conclusion:

A surprising majority of surveyed organizations – 88% of respondents! – have experienced a firmware-level attack in the last two years. And yet there is a clear discrepancy between the state of awareness around firmware security and the perception of knowledge that IT departments have. This creates a challenge in any environment, but with firmware this discrepancy is all the more severe: the critical role firmware plays in enabling and defending our technology supply chains makes it the most attractive target for our adversaries. At the same time, the defender's level of overconfidence leaves them vulnerable, unaware and unable to truly improve upon current realities. The result? The firmware back door is wide open to hackers and cyber criminals.

Whether organizations truly understand the threat or not, firmware-level attacks are on the rise. Organizations like CISA, the U.S. Cybersecurity and Infrastructure Security Agency, expect them to become even more prominent: their Known Exploited Vulnerabilities (KEV) list **shows firmware-based exploits leading the pack** over all other kinds of exploits in the last 10 years. Indeed, it appears that adversaries are better at attacking firmware than defenders are at protecting it.

However, the current state of play doesn't have to remain the same moving forwards. Organizations have an opportunity to upskill staff, increase awareness and knowledge, and improve firmware security throughout their supply chains, from manufacturers and OEMs to enterprise customers and end users. It is often the case that a greater level of investment and human resource allocation is needed to make change and the same applies to firmware. As organizations prioritize firmware security they will benefit from not only decreased risk of cyber breaches, but also reduced attack surface, shortened reaction times, more resilient supply chains and more successful security audits.

Firmware doesn't need to be the weakest link in our digital supply chains - support is here. The time to act is now.

Methodology:

Eclypsium commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this whitepaper is based. A total of 350 IT security DM respondents, from organizations with a minimum of 1,000 employees, were interviewed in May 2022. Respondents were targeted in the US (150), Canada (50), Singapore (50), Australia and New Zealand (50) and Malaysia (50). All respondents were from organizations in the financial services sector.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated the results discussed are based on the total sample.

About Eclypsium

Eclypsium's cloud-based platform identifies, verifies, and fortifies firmware in an enterprise's digital supply chain: in laptops, servers, network gear, and connected devices. The Eclypsium platform secures devices against firmware threats and critical risks, and by patching firmware across the entire hardware fleet. For more information or to inquire about firmware and supply chain risk assessments visit **www.eclypsium.com**

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit **www.vansonbourne.com**