Separated by a common language:

Is the C-Suite able to truly decipher and act upon the real threat of cyber-attacks?

kaspersky

Contents

Introduction

"Language is very powerful. Language does not just describe reality. Language creates the reality it describes" **Archbishop Desmond Tutu**

Language is important. For a start, without language we wouldn't have...language, or anything that is dependent on language for that matter.

Language has enabled the study of ancient philosophy, scientific breakthroughs, computer programming, or even sending WhatsApp messages to your friends and family. And in the same way that any language transmits and mediates everything from social norms to the creation of culture, shared histories, mythologies, religions and art forms, cyber security too, has its own language.

It is common knowledge that cyber security threats are occurring every day, arriving in all shapes and sizes, and speaking a variety of technologically and geographically different languages. Internet forums, media publications, and news channels around the world feature news of the latest attacks which, in written or verbal form, are a mix of acronyms, jargon, and idioms acting as shorthand for those in the know, but which might seem bewildering to interpret for anyone without prior experience of working within the sector.

The terms "deep web" and "dark web" are often used interchangeably, conjuring evocative images of gangs gathering to buy credit card numbers, drugs, guns, counterfeit money, and hacked account details that can be used to break into people's computers or even assume their identities entirely. The reality is that these are different things. The "deep web" simply referring to anything on the internet that is not indexed by, and therefore accessible via, search engines like Google.

The "dark web" is a subset of the deep web that is intentionally hidden and requires a specific browser to navigate. There are legitimate reasons why some people may wish to make information available in the way that cannot be indexed as it is in the surface web. For example, it plays an important role in supporting oppressed human rights activists, journalists, etc. who lack free speech in their own country. However, it is also used for conducting illegal activity.

Given the esoteric nature of the illegal transactions happening there, it is impossible to interpret and understand without speaking the language of cybercrime. The sharp end of the dark web – the malware, distributed denial of service, botnets, Trojans, phishing scams and keyloggers – are well-publicised, but what actually are they, and if I'm responsible for running a business, how much do I really need to know to protect that business?

As the world continues to re-engineer its business practices amid ongoing geopolitical, environmental, and economic upheaval, intelligence into the nature of these cyber security threats at the highest level of business has never been more important. The reality of an increasingly digitised world meaning that almost every business decision and transaction now

has a cybersecurity dimension. Priorities have shifted from firewalls and identity management to strategic challenges like brand trust, product security, and resiliency.

Kaspersky is a global company with threat intelligence experts active in every region. The business has used this unique experience to undertake extensive research into how the evolving nature of cybersecurity threats is being interpreted by a C-suite challenged with defending its businesses against them.

Are they focusing on and discussing the right threats in the boardroom? Have they invested in the right tools to defend against those threats? Are they even aware of the threats to their businesses which carry the most danger?

Our findings exclusively reveal a C-Suite that is mostly aware of how often their businesses are being attacked, but that the language and terminology that is being used to describe cyber security threats is simply too opaque for them to interpret and isn't resonating. This means that the **C-suite is often finding itself in a position where they are having to make business critical decisions without a clear picture of their unique threat landscape and the risk it poses to their organisation**.

The following report highlights both significant leaps in cybersecurity awareness in the boardroom on one side, with clear areas for improvement on the other. The findings uncover that while there is no shortage of information on the topic and concern on the part of the C-Suite, crucially there is a clear lack of available and actionable intelligence.

Methodology

A total of 1,800 interviews with C-Level decision makers in large enterprises of 1,000+ employees were conducted across 12 countries in September 2022 (UK (200), France (200), DACH (Germany - 100, Austria - 50, Switzerland - 50), Benelux (Netherlands - 100, Belgium - 100), Spain (200), Portugal (200), Italy (200), Romania (200) and Greece (200). Respondents were asked about cybersecurity within their organisation, the measures they take to protect themselves, and the barriers they face as a management team.

Throughout this report Chief Executive Officers, Chief Operating Officers, Chief Marketing Officers, Chief Risk Officers, Chief Investment Officers, Chief Financial Officer, Chief Compliance Officers, and Chief Information Officers are referred to as the 'C-suite'.

Key Findings

The C-Suite knows that cybersecurity attacks represent the biggest threat to its businesses, but the bigger the company, the less important it is at board level:

- From the perspective of the C-suite, the biggest risks currently facing businesses are cybersecurity attacks (49%), ahead of economic factors such as inflation and interest rates (37%)
- With that in mind, just over half (51%) of C-Suite respondents stated that cybersecurity is now always an agenda item for their board meetings, with 2 in 5 (43%) say it sometimes is.
- Yet the bigger the company, the less aware they are of cyber threats with only 35% of companies with 5,000+ employees admitting they knew of attacks compared to 52% in companies of 1,000-1,999 employees.

Although cybersecurity is a clear concern for the C-Suite, the language being used to describe threats is severely impacting its ability to understand and act on them:

- Despite cybersecurity being a clear concern to the C-suite, almost half (48%) of C-Level security specialist respondents stated that **security jargon and confusing industry terms are the biggest barrier** to the broader management team's understanding of cybersecurity and how they should tackle it.
- 38% of C-level executives surveyed stated that they **found basic cybersecurity terms like Malware, Phishing and Ransomware to be confusing.**
- Furthermore, budget restrictions (47%), and insufficient training (43%), round out the top three biggest barriers the C-suite faces in understanding cybersecurity

Although there are some geographic differences, the C-Suite is generally still reliant on social media, blogs, and news resources to gather intelligence:

- In a bid to build understanding, almost half (47%) of the C-suite stated that they are **reliant on social media, cybersecurity blogs, and publicly available news** resources to gather intelligence on cybersecurity trends for discussion in the boardroom.
- Across all the countries surveyed it was the Spanish C-Suite (34%) that **was most likely to turn to the dark web** to gather cybersecurity intelligence for discussion in the boardroom.

Yes, we know cybersecurity is our biggest problem… it just often isn't a priority boardroom topic.

Over the past 12 months cybersecurity has continued to dominate global headlines, with high profile attacks resulting in a loss of money, reputational impact, and vulnerabilities on a human level. It should therefore be no surprise, that our research finds that nearly all (99%) C-Level executives interviewed are now aware of how often their businesses are being attacked by threat actors.

Of those respondents, 52% of C-Level executives in companies of 1,000-1,999 employees claimed that they were very aware of how often their business was being attacked, whilst just 35% in companies of 5,000+ admitted the same. Furthermore, almost half (49%) of the C-Suite interviewed admitted that cybercrime is now the biggest threat to their business, well ahead of major economic factors such as rising inflation (37%), regulation and compliance (35%), and competitors (29%).

Despite this clear understanding of the prevalence of the cybersecurity threat, 43% stated that cybersecurity was only sometimes an agenda item during board meetings. Of those, 1 in 7 (14%) of C-Suite respondents in companies with 5000+ employees stated that cybersecurity is rarely an agenda item for their management or board meetings. This compares to just 3% of C-Suite surveyed in a company size of 1000-1999 employees or 2000-2999 employees.

These findings highlight that the bigger the organisation, the greater the potential disconnect between those with technical knowledge and the board, suggesting a failure to articulate cyber-security issues in business terms, in a way that's meaningful for executives.

The C-suite considers cybersecurity to be the biggest problem facing their businesses, with nearly half considering it more of an issue ahead of current economic factors like rising inflation and the impact that has on costs to the business. However, the larger the organisation the less likely it is for C-Level executives to have a deep awareness of the major cybersecurity issues and the impact they can have on the business, or for it even to be regularly discussed in the boardroom.

	UK	France	DACH	Benelux	Spain	Portugal	Italy	Romania	Greece
Cybersecurity attacks	57.0%	46.0%	61.0%	52.0%	45.5%	51.5%	44.0%	45.0%	43.0%
Economic factors	30.5%	37.0%	35.0%	44.0%	40.5%	33.0%	41.0%	45.5%	28.0%
Regulation/ compliance	27.0%	36.0%	35.0%	35.5%	38.5%	35.0%	34.5%	37.0%	34.0%
Natural disasters	26.0%	36.5%	29.0%	30.0%	40.5%	26.5%	31.0%	32.5%	26.0%
Competitors	30.5%	30.0%	26.5%	30.0%	31.5%	30.5%	28.0%	25.0%	31.0%
Environmental issues	26.0%	31.5%	25.0%	32.0%	37.0%	20.0%	29.5%	29.0%	28.0%
Industrial action	29.5%	30.0%	29.0%	23.0%	27.5%	29.5%	26.00%	26.0%	34.0%

Fig 1. Biggest risks/threats facing business continuity

Whilst it is inevitable that the larger the footprint, the more numerous the threat vectors – for instance, more people, and more systems to protect – this suggests that many organisations are playing catch-up with their own growth. At the top level, any business faces many competing priorities in terms of recruitment, customer acquisition, infrastructure maintenance and so on, but the results point to a bigger disconnect within larger organisations. A disconnect between the C-level and their ability to truly understand the implications of their biggest challenge: cybersecurity.

Understanding the implications of a successful attack on business operation, the financial impact and how reputation can be affected by a breach is no longer optional for high-powered decision makers. It is worrying to see the boards of large organisations failing to appreciate how important cybersecurity and threat intelligence are for their business, highlighting a disconnect between savvy technologists and decision-making executives. Whilst the board does not necessarily need to understand the complex intricacies of cybersecurity as such, they must easily comprehend the impact that threats can have on the business.

David Emm
Principal Security Researcher, Global Research and Analysis Team, Kaspersky

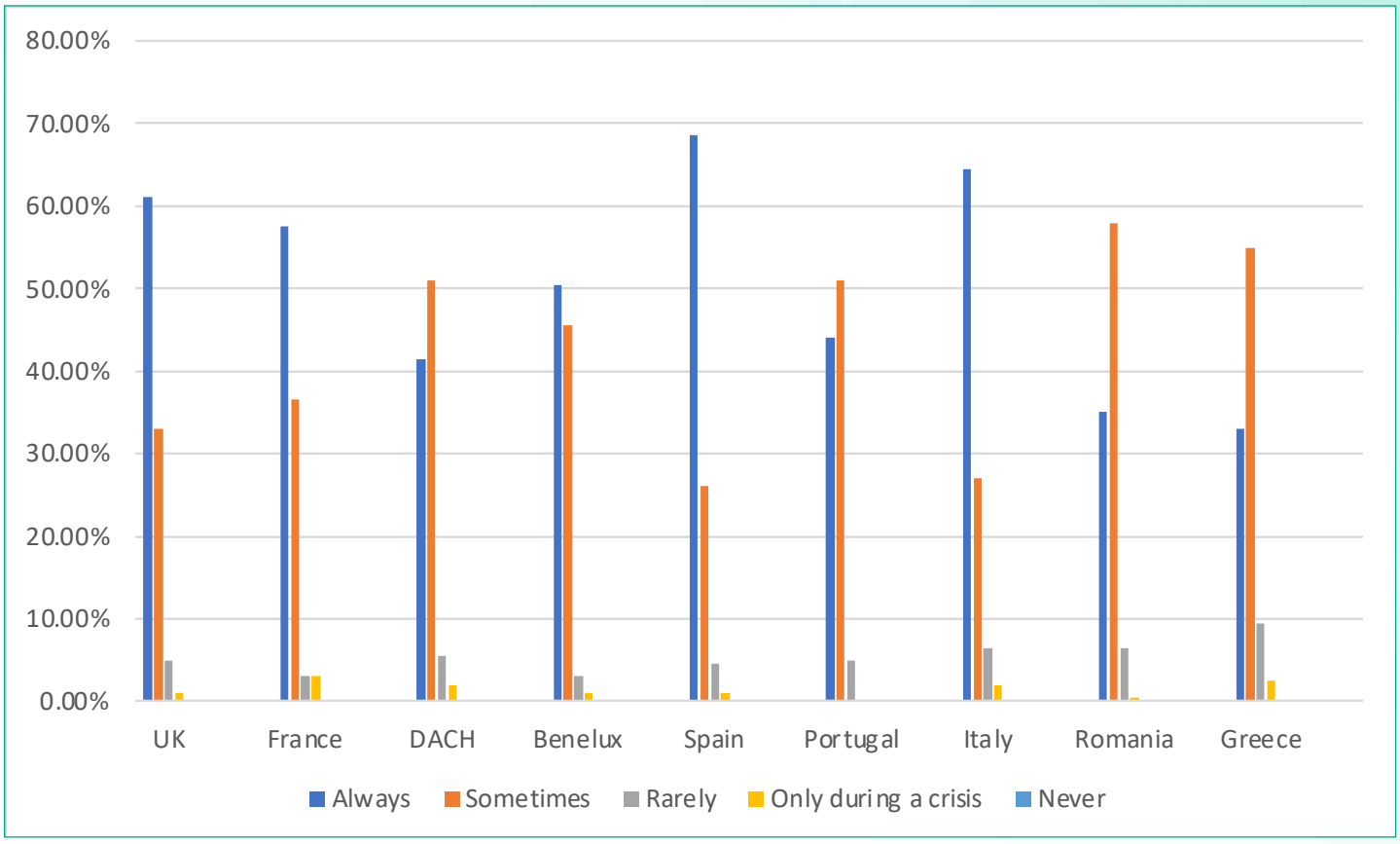

Fig. 2 Is cybersecurity an agenda item for your management or board meetings?

The biggest obstacle we face is not knowing what any of this really means

Despite cybersecurity being a clear concern to the C-Suite and their businesses, almost half (48%) of C-level security, compliance, and risk specialists believe that jargon and confusing industry terms are currently presenting the biggest barrier to their broader management team's understanding of cybersecurity and, most importantly, what they should do about it.

This is particularly apparent across the DACH (Germany, Austria, Switzerland) region (47%), Portugal (47%), Spain (44%) and UK (42%) with C-level security specialist respondents stating that jargon is the main barrier for their management team's understanding of the most pressing cyber security threats.

To illustrate this point more vividly, **38% of all those surveyed stated that they found basic cybersecurity terms Malware, Phishing and Ransomware to be confusing**. Slightly more technical language used such as 'Zero Day Exploits' and 'Suricata rules' saw similar levels of confusion with 39% of respondents claiming to not fully understand these terms.

Across the countries, C-Suite executives surveyed in Italy are more likely to find the terms Malware, Phishing, and Ransomware confusing, with exactly half of respondents (50%) confessing that these terms were not entirely understood. Respondents in France were most likely (47%) to find the term 'Nation State Attack' confusing.

Globally, it is the budgetary restrictions (47%) put in place by the business and insufficient training (43%) within the management team that rounded out the top three barriers to cybersecurity success. Of the countries asked, it was C-Level executives based in the UK (56%) and France (52%) who stated that it was budget most holding them back. Whereas in Italy and DACH, 42% stated that insufficient training was the reason.

Simply put, Kaspersky research findings reveal that there are significant obstacles to the C-Suite developing a more comprehensive understanding and awareness of the most important cybersecurity issues facing their businesses. And it is the language that is being used to transmit and mediate these issues that is currently inhibiting an organisation's ability to develop a culture of cybersecurity best practice, share knowledge, and, ultimately, institute actionable intelligence.

Our data suggests that cybersecurity, to differing extents depending on geographic location, is an industry that speaks to itself, using language that can be impenetrable to those without a specialist security background. Awareness and understanding can follow but for this to happen a bridge is required to interpret the lexicon and verbiage used throughout the dark web and into the commonly understood conventions of the boardroom.

Cyber Threat Snapshot:

Malware	An umbrella term for computer programs designed to be installed on a person's computer and inflict harm upon it in multiple ways. A simple contraction for "malicious software", common malware includes viruses, worms, Trojans, spyware, adware, and ransomware.
Phishing Attacks	Phishing is a form of social engineering employed in both cybercrime and APT attacks, in which targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to compromise a device and gain access to sensitive data. This data can also used for identity theft for financial fraud purposes.
Nation State Attacks (APTs)	These are high-profile attacks aimed at national infrastructures, with a view to weakening the economic, military, or political sphere of a given country.
Ransomware Attacks	Malicious software that encrypts data or blocks access to it, demanding that the user pay for unlocking or decrypting the data. Different varieties of malware target desktop systems and mobile devices.
Supply-chain attacks	A supply chain attack targets elements in the supply chain before sale to the end user. An example of such an attack is modifying a product update so that malware is delivered to all customers of that product
Zero Day Exploit	This term is used to describe exploit code that has been written to take advantage of a vulnerability before the software vendor knows about it and has had the chance to publish a patch for it. The result is that would-be attackers are free to exploit the vulnerability, unless proactive exploit prevention technologies have been implemented to defend the computer being targeted by the attacker.
Indicator of compromise (IoC)	This is an object or activity that, observed on a network or on a device, indicates a high probability of unauthorized access to the system — in other words, that the system is compromised. Such indicators are used to detect malicious activity in its early stages as well as to prevent known threats.
TTPs	TTPs stands for tactics, techniques, and procedures. This is the term used by cybersecurity professionals to describe the behaviours, processes, actions, and strategies used by a threat actor to develop threats and engage in cyberattacks.
Mitre ATT&CK rules	Adversarial Tactics, Techniques & Common Knowledge is a knowledge base describing cybercriminal tactics and techniques based on real-world observations. The MITRE Corporation created the knowledge base in 2013 and the project's purpose is to develop a structured matrix of cybercriminal techniques to facilitate cyber incident response.
Suricata rules	Suricata rules are the de facto method for sharing and matching threat intelligence against network traffic.
MD5	A hashing algorithm that converts a dataset of arbitrary size into a hash — a pseudorandom sequence of fixed-length characters. The result is a kind of identifier for the encrypted data array. MD5 is used to verify the authenticity, integrity, and immutability of any set of characters (for example, computer code). If the checksums match, it means the file has not been modified. Some operating systems use MD5 to store passwords.
YARA	A tool primarily used in malware research and detection that provides a rule-based approach to create descriptions of malware families based on textual or binary patterns.

Wider glossary available at: https://encyclopedia.kaspersky.com/glossary/

Communication shouldn't be hindering cybersecurity. What our findings highlight, is the importance of strategic planning, budgeting and sourcing knowledgeable staff from the top down, but also channelling back relevant incidents from the bottom-up in an understandable, clear fashion, without the need to resort to woolly language or complex industry jargon. A functioning two-way communication is essential for a functional long term operation.

Christian Funk
Head of DACH Unit, Global Research & Analysis Team, Kaspersky

	UK	France	DACH	Benelux	Spain	Portugal	Italy	Romania	Greece
Budgetary restrictions	56.5%	52.0%	46.5%	47.0%	47.5%	42.5%	42.5%	43.5%	45.5%
Insufficient training	43.0%	51.5%	42.0%	40.5%	55.0%	39.5%	42.0%	42.5%	31.5%
Jargon/ confusing industry terms	42.0%	40.0%	46.5%	43.0%	44.0%	46.5%	41.0%	45.0%	31.5%
Lack of tools	35.0%	37.5%	40.5%	49.5%	45.5%	35.0%	44.5%	37.5%	47.0%
Lack of time	37.5%	35.5%	28.0%	41.0%	42.0%	30.0%	40.0%	35.0%	46.0%
We do not face any barriers	0.5%	2.5%	2.0%	0.5%	1.5%	1.0%	8.0%	0.0%	0.0%

Fig 3. What, if any, barriers do you face in your management team having a full and extensive understanding of cybersecurity?

Ok, so what is a Malware?

It is important to first understand what organisations are up against.

Originally contrived as a US Department of Defense project in the early 1990s to develop an anonymised and encrypted network that would protect the sensitive communications of US spies, dark webs have since taken on a life of its own. Although it comes in different variations based on their technical implementation and their respective "goals", it can be defined as a highly sophisticated and complex network of off-grid forums, chat rooms, file and image hosts, and commercial marketplaces.

For people living under oppressive regimes that block large parts of the internet or punish political dissent, it is important to note that dark webs are a lifeline that provides access to information and protection from persecution. But for the overwhelming majority of the dark web that is used for nefarious activities, the sophistication and complexity of dark webs provides the ideal environment for criminals to thrive, away from the prying eyes of the authorities.

Dark webs do not have standard webpage indexing by surface web search engines, meaning that Google and other popular search tools cannot discover or display results for pages. Depending on the type of dark web, it can use virtual traffic tunnels via a randomised network infrastructure which renders the dark web inaccessible by traditional means. To the untrained outsider it is an impenetrable fortress.

In a bid to educate themselves against the threat being incubated and unleashed from this dark web, **our research finds that nearly half (47%) of the C-Suite**

is predominantly reliant on news stories, industry blogs, and social media feeds to gather insight into cybersecurity topics that can be discussed during board meetings. This method of cybersecurity education is an important way of understanding the threats which are facing businesses; however, it needs to be part of a layered approach to education and awareness.

Publicly available information on industry blogs and media resources provides an important way to keep up to date with the latest issues, but a reliance on consuming information about the most 'popular' trending new stories can limit the C-Suite from developing a holistic understanding of the threats present to them and how to stop them.

Just 40% of C-level respondents stated that they are turning to external vendors/experts to gather intelligence on the latest threats emerging from the dark web, preferring instead to develop their knowledge using publicly available information. Although well over 2 in 5 (46%) C-Suite surveyed are using private threat intelligence sources to gather intelligence -and discussing them during boardroom meetings- another 40% is relying on internal resources to decipher emerging threats from dark webs and subsequently illustrating the findings during board-level meetings.

Of all the countries surveyed, C-Suite executives surveyed in Spain stated that they are most likely to be using dark web threat intelligence and discussing it during board meetings (50%), while on the polar opposite, C-Suite surveyed in the UK is the least likely to do so across Europe (34%).

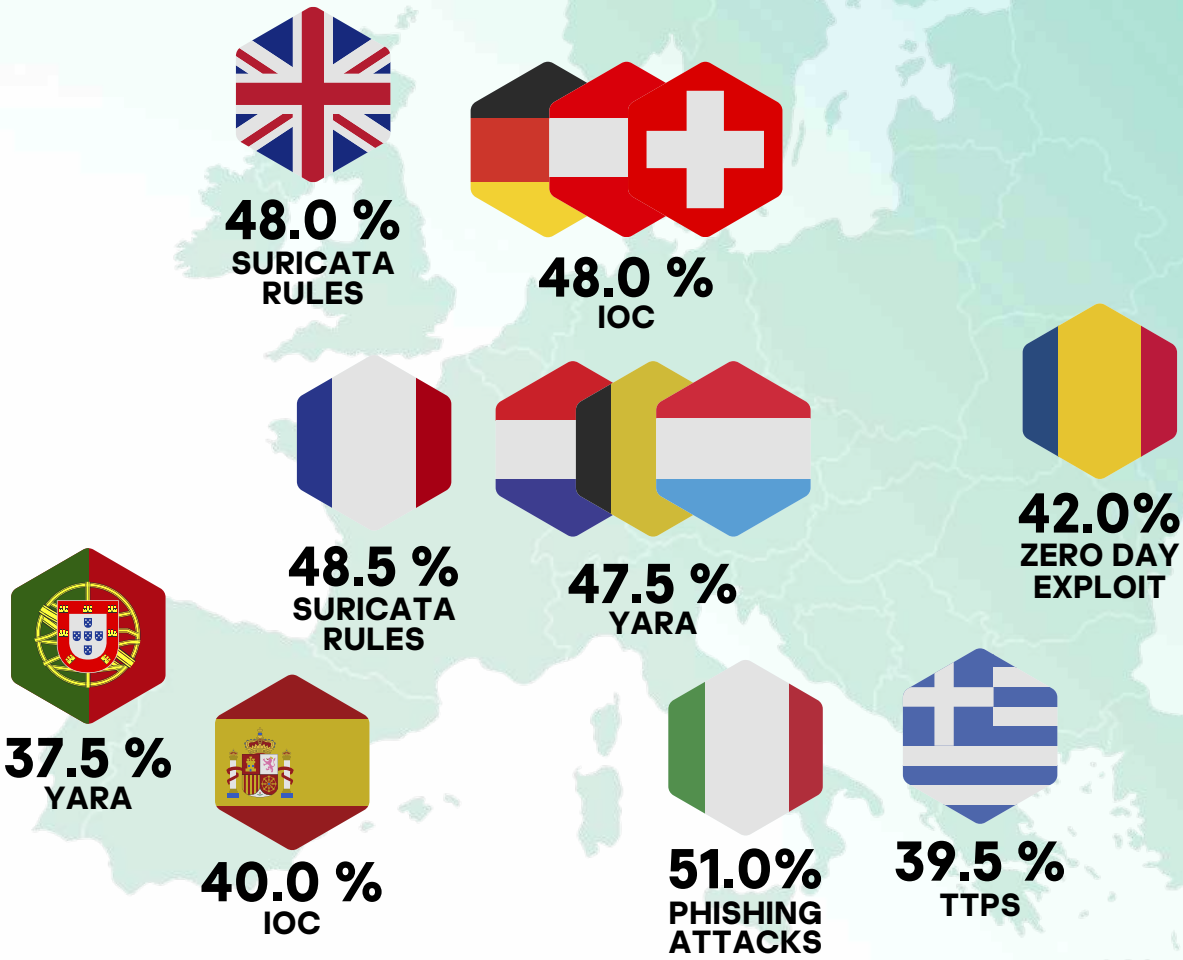

Fig 4. Percentage of terminologies that executives struggle to understand the most

Cybersecurity: who are you going to call?

The research paints a picture of a C-Suite that needs help in understanding the security threats that are facing their businesses every day. The threat landscape is a complex and ever evolving place consisting of some of the most highly motivated and technologically sophisticated criminals on the planet. It is one thing being aware of the cyber threats which are out there and entirely another to understand them.

As the threat landscape has evolved, so has the language which is being used. As we have seen from the research, this evolution, in many cases, is outstripping the ability of businesses to keep up. Competing commercial priorities, rapidly changing economic and social environments, and competitive pressures have not eclipsed the awareness of the threat posed by cyber-attacks, but an inability to understand the nature of the threat and then act upon it has seen cybersecurity drop down the agenda during board meetings.

The consumption of publicly available resources, and more budget being made available for training, will help to develop awareness. The reality, however, is that without solid expertise to identify, analyse and cross-correlate cyber threats, organisations are only half-arming themselves against the threat. At the core of this approach is an interpreter or partner who can not only speak the language of cybercrime, but also understand how the privacy and anonymity that provides protection for criminals can be used against them to develop a rapport and then extract critical intelligence,

For more information on how businesses can protect themselves against cybersecurity threats get in touch with the Kaspersky Threat Intelligence team here.

Other factors inhibiting cyber security awareness

- 41% of C-Level executives believe that a lack of tools available to them was a major barrier to having a full and extensive understanding of cybersecurity and the threats they possess.
- According to the C-suite, IT Managers are most likely to present threat intelligence information during their board meetings (51%), followed by CISOs (45%), external cybersecurity vendors (44%), non-technical written executive summaries (31%) and finally, Partners (25%).
- Respondents using and discussing public threat intelligence sources (open source, social networks, cyber blogs) in the boardroom are most likely to say they are doing so to circumnavigate disruption (56%), rather than to circumnavigate cost issues (53%) or because it is the most / one of the most reliable (22%).