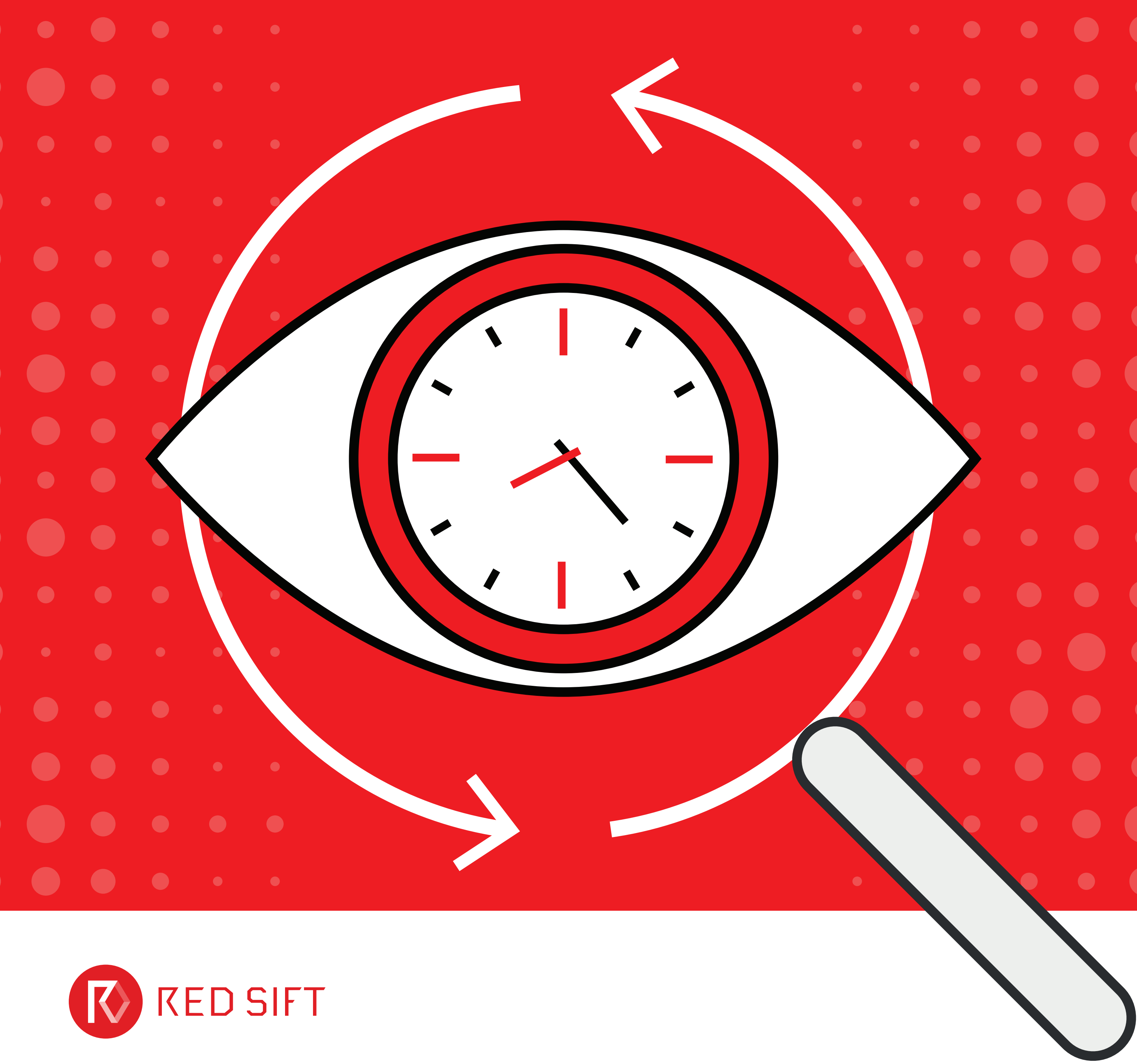


RED SIFT

State of Cyber Resilience 2023

Analyzing the readiness of organizations worldwide to withstand and recover from cyberattacks

State of cyber resilience 2023

Introducing the Red Sift State of Cyber Resilience Report. This comprehensive report unveils the latest insights into the evolving landscape of cybersecurity resilience. Drawing from a global survey of top executives across diverse industries, the report delves deep into the challenges and opportunities faced by organizations in safeguarding their digital assets. It sheds light on new developments in cyber resilience strategies, highlighting innovative approaches and best practices that are shaping the future of cybersecurity. Moreover, the report underscores the critical role of emerging governance, risk, and compliance frameworks in ensuring organizations remain adaptive and resilient in the face of ever-evolving cyber threats. In an era where digital risks are continuously evolving, this report will serve as an indispensable resource for decision-makers seeking to fortify their cybersecurity defenses and stay ahead of the curve.

Executive introduction

As we navigate the intricate digital terrain of today's interconnected world, it is imperative that we acknowledge the paramount significance of cyber resilience. We observe that cybercrime has evolved into a significant drag on economic growth and a global security concern. The attack surface continues to grow as well, as more services are brought online alongside our expanding collective dependence on digital infrastructure in every aspect of our lives. The global landscape of cybersecurity is evolving at an unprecedented pace, with threats becoming more sophisticated and prevalent. Cyber resilience allows organizations to withstand and recover, even while facing adversity.

Lessons on resilience are also world news. Ukraine's valiant efforts to strengthen its cybersecurity ecosystem serve as instructive examples for nations and organizations, detailing the criticality of proactive measures to enable resilience.

Red Sift's commitment to cyber resilience goes beyond safeguarding data and services; it's about ensuring the universal ability to adapt, withstand, and recover from mounting challenges. In an era where digital transformation is integral to global operations, our dedication to achieving cyber resilience drives us to not only respond to threats but to anticipate and preempt them. As this report details, it is that proactive approach that strengthens our collective foundation, nurtures innovation, and safeguards trust for a safer and more secure cyberspace.

With a steadfast focus on cyber resilience, we stand ready to face the uncertainties of the digital age, fortifying organizations against the evolving landscape of cyber threats and embracing the opportunities that lie ahead.

Proactive cybersecurity is the shield that guards your digital fortress before an adversary strikes. Resilience is what turns setbacks into stepping stones.

Rahul Powar
CEO
Red Sift

Table of Contents

Introduction

Cyber resilience transcends reactive measures and necessitates embracing a proactive mindset across the enterprise. It is about not only bouncing back from incidents but adapting and progressing in advance of cyber threats. As cyber threats evolve and become more pervasive and sophisticated, organizations must continuously adapt their strategies and approaches to stay ahead. By embracing resilience, integrated risk management, risk-aware culture, and enabling technologies, organizations can mitigate risks, respond effectively to incidents, and maintain their operations and trust in the face of ever-present cyber challenges.

Technology can be both a challenge and a solution in cybersecurity, simultaneously enabling adversaries while also giving an edge to defenders. Most critically, technologies should be thoughtfully adopted and implemented, taking into consideration their fit with the organization's risk profile and objectives. No matter the mix, resilience is best accomplished through a comprehensive cyber risk management approach.

The entire C-Suite – not just CISOs – are increasingly recognizing the value of shifting from a purely defensive stance to a strategic and forward-looking approach. Such an approach involves continuously assessing risks, developing comprehensive incident response plans, conducting regular drills and simulations, and fostering a culture of cybersecurity awareness throughout the organization.

Organizations need to cultivate resilience by preparing for a variety of scenarios and solving for priority risks, thereby ensuring that they can withstand and recover from cyber incidents while minimizing their impact on operations, reputation, and stakeholders. To do so effectively, organizations must also leverage cutting-edge cybersecurity technologies, such as advanced threat detection tools, artificial intelligence, machine learning, and encryption, to fortify their defenses and increase resilience.

Security experts are also actively working to create risk-aware cultures that understand and embrace the criticality of cyber risk. All employees, from the leadership down to individual contributors, need to be educated about cybersecurity best practices and risk implications. Encouraging a culture of security-consciousness and accountability fosters an environment where everyone plays a role in protecting the organization.

After all, cyber risk is no longer confined to the IT department, it permeates every facet of an organization. A comprehensive cyber risk management approach integrates cybersecurity considerations across all levels and functions, aligning with business objectives and strategies, holistically identifying, assessing, mitigating, and monitoring cyber risks proactively.

Scope of the Red Sift State of Cyber Resilience report

This report covers a wide array of significant events and data points in the cybersecurity landscape that portend changes for resilience. These junctures include new technologies, processes, organizational approaches, regulations, and frameworks. The State of Cyber Resilience (SCR) Report draws on thorough evaluation of Red Sift's first cyber resilience survey and its results. Further resources for the report include highlights of expert interviews we conducted in 2023 and the analysis of proprietary data to provide a holistic view of the global cyber resilience.

Key Findings

1. Evolving threat landscape

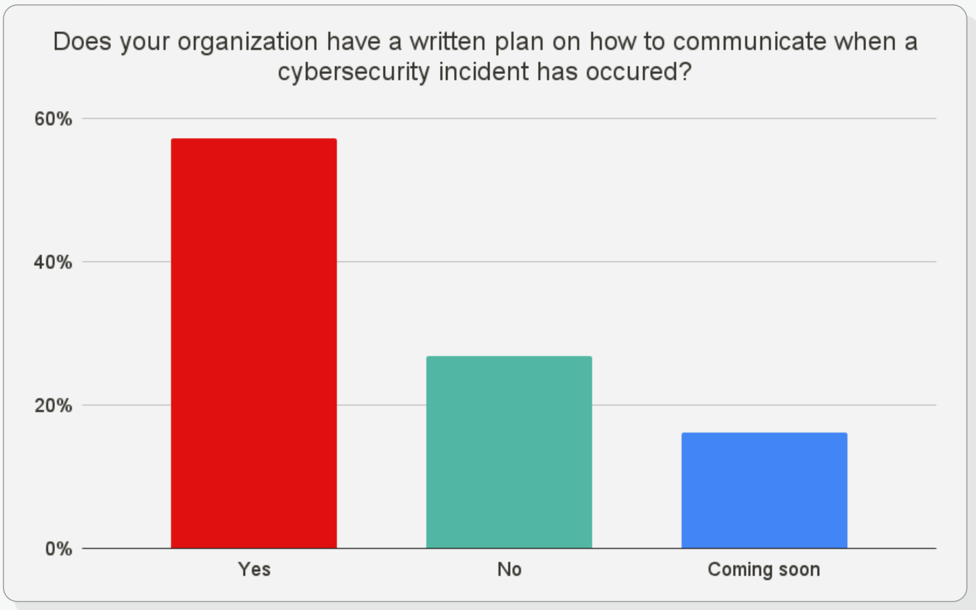
The threat landscape in cybersecurity is undergoing rapid and complex evolution, presenting unprecedented challenges for organizations and individuals alike. As technology advances, so do the tactics, techniques, and procedures employed by malicious actors. The blurring of boundaries between physical and digital domains is increasing risks such as ransomware attacks on critical infrastructure or operational technology. Ransomware and business email compromise still lead the pack, but trends in ongoing digital transformation and remote work, much of which was triggered by global events, are shifting the focus of attackers towards exploiting vulnerabilities in cloud services, operational technology, remote access, and collaboration tools. In this dynamic environment, cybersecurity measures are being pushed to adapt and innovate at a pace that matches, if not exceeds, the agility of cyber threat actors.

2. Pursuing organizational readiness

While many large corporations have invested significantly in cybersecurity, small and medium-sized enterprises (SMEs) often lack the resources and capacity to onboard expertise to meet changing requirements for cybersecurity, not to mention defend against advanced threats. But as our research shows,in many cases whether it's a large corporation or SME the basics in cybersecurity are still not being done. For example, the results from our research suggest that nearly half of the organizations surveyed have yet to prepare written plans to communicate when an incident has occurred. Further complicating the issue of organizational readiness, our survey indicates that a significant number of organizations are still not conducting periodic or consistent risk assessments, leaving them vulnerable to surprise.

3. Changing regulatory environment

Governments are becoming more proactive in issuing guidance and legislating cyber policies. The global landscape of cybersecurity is witnessing positive transformation through a wave of regulatory changes. These regulatory changes are driving organizations to prioritize data protection, privacy, and risk management. However, thus far, there are mixed results. In some cases regulations may be misaligned between countries, creating challenges for multinational corporations even within regulatory blocs like the European Union (EU). Our research also suggests that more cybersecurity regulations are aimed at achieving some measure of resilience and new regulations will put further onus on companies – particularly IT companies – to help those dependent on them achieve resilience.



4. Expanding frameworks

Cybersecurity guidance and frameworks are undergoing dynamic changes to adapt to the evolving threat landscape and the increasing complexity of digital ecosystems. Governments and framework developing bodies around the world are recognizing the paramount importance of a secure digital environment and are taking proactive steps to expand existing frameworks to enhance cyber resilience. As technology advances and organizations become more interconnected, widely adopted frameworks are augmenting their scope to encompass a greater range of risks and challenges. Our research finds notable shifts in the integration of risk-based approaches, emphasizing the need to prioritize security measures based on the potential impact of threats, the need for transparency for stakeholders, and expanding the understanding of cyber as an enterprise-wide risk. As we detail in this report, the the United States, the EU, and industry groups have made significant strides in new frameworks for resilience.

5. Understanding the criticality of people in cybersecurity

Human factors play a pivotal role in the realm of cybersecurity, underscoring the critical interplay between technology and human behavior. Despite technological advancements, humans remain both the weakest link and, equally, the most essential component in the security chain. Understanding cognitive biases, promoting critical cybersecurity awareness, and providing effective blame-free training are key components in mitigating human-related vulnerabilities. As cybersecurity threats continue to evolve, recognizing and addressing the human element is essential for building resilient defense mechanisms that account for the complexities of human behavior within the digital landscape. The global shortage of cybersecurity professionals continues to be greater than 3 million people worldwide. More challenging still, organizations that suffer serious cybersecurity breaches often see significant numbers of hard-to-replace staff depart.

Resilience is crucial for economic and national security. Recent ransomware attacks such as the Colonial Pipeline incident have demonstrated that even a single attack can disrupt supply chains necessary for national vitality."

Mihoko Matsubara
Chief Cybersecurity Strategist
NTT

Embracing resilience

For many security leaders today, it can feel like they are working against a stacked deck. Understaffed and stressed security teams, the prospect of AI making cybercrime yet more prevalent and efficient, and a rapidly changing regulatory landscape are just three pressing factors C-Suite leaders need to incorporate into an organization's security strategy.

C-Suite leaders can no longer look at cybersecurity as something that is handled in a silo, with individual threats that only require sufficient focus to survive one-off attacks. Instead, they are seeing the need to muster people, processes and technology holistically to achieve cyber resilience.

So what is cyber resilience?

We offer the definition that cyber resilience details an organization's ability to anticipate, respond to, and recover from cyber attacks while continuing to operate effectively.

Resilience encompasses a comprehensive set of strategies, processes, and technologies that mitigate the impact of cyber incidents and enable rapid and efficient recovery.

Conceptually, this may seem simple and straightforward enough. But, if it were so straightforward, why has it taken so long for holistic resilience strategies to become the norm?

Historically, conversations around cybersecurity have been reactive and tactical. 'How did the breach happen?' 'How much is it going to cost to remediate?' 'How are we going to prevent this from happening again?' 'Does our insurance cover it?' and, of course, 'Whose fault was it?'.

But a sea change is underway. Leaders are recognizing that a smoothly operating organization requires the resilience to anticipate, adapt, and overcome.

> *Security leaders no longer have the luxury to be reactive to breaches. Cyber resilience now entails enlisting solutions that can anticipate, warn, and mitigate cyberthreats before an attack has the opportunity to infiltrate an organization's network."*

Ivan Ristic
Chief Scientist
Red Sift

Why resilience, why now?

Cyber threats have transcended the realm of simple viruses and malware to encompass zero-days and sophisticated supply chain attacks from nation-states and their proxies to the now quotidian but nonetheless damaging threats emanating from organized cybercrime syndicates. Radical advances in artificial intelligence promise more insight and better defenses, but also come with the peril that adversaries may gain still greater advantage.

- The costs of data breaches are increasing. IBM reports that the average cost of a data breach has reached $4.45 million in 2023[i]
- According to Check Point's 2023 Mid-Year Security Report criminal actions have ballooned in the second quarter of 2023 with an 8% surge in global weekly cyberattack – the highest volume in two years.[ii]
- Microsoft's Cyber Signals report notes a 78% increase in disclosures of high-severity vulnerabilities from 2020 to 2022 in industrial control equipment produced by popular vendors.[iii]
- The proliferation of interconnected devices through the Internet of Things (IoT) is radically expanding the attack surface, leaving critical infrastructure, data streams, and supply chains vulnerable. The International Data Corporation (IDC) estimates there will be 55.7 billion connected IoT devices by 2025.[iv]
- Fallout continues from the spectacular MOVEit breach, with over 1,000 organizations now known to have been caught up in the breach and over 60 million individuals affected.[v][vi]

Many organizations have embraced risk reduction methods that shift some risk in cybersecurity to another party. But with growing concern about large-scale and cascading attacks, risk transfer is now longer a viable option for many. As such, organizations can no longer wait for disaster to strike or, when it does, depend exclusively on insurance to prop them up.

The insurance industry is deeply challenged by the scale and scope of cyberattacks, which, as MunichRe notes in its report Cyber Insurance: Risks and Trends 2023, now includes geopolitical risks that went largely unimagined a decade ago[vii]. The challenges are such that Mario Greco, chief executive at global insurer Zurich, has gone so far as to suggest that cybersecurity might become uninsurable.[viii]

Cyber insurance, which operates like other types of insurance, requires that the insured has made a fair representation of the risks to their insurance company. In the UK and Ireland, this representation is made before the contract is entered into, while in the US the insured is under a continuing obligation to disclose.

Concomitant with the changing threat landscape, governance in cybersecurity is now undergoing a paradigmatic shift from reactive security to proactive measures that promise greater resilience. Released in 2023, the new draft NIST Cybersecurity Framework 2.0 is emblematic of this shift. NIST recognized the importance of a foundational layer to address non-technical and operational issues and, as such, conceived of a major addition to its well-established framework: "Govern[ix]." This new pillar is designed to emphasize that cybersecurity is a major source of enterprise risk, elevating its importance and signaling to all stakeholders that corporate governance in cybersecurity is a critical component of resilience.

As we aim for resilience, ensuring best practices and mitigation for policy holders is a critical role for insurers. The challenge of insurability is a great opportunity for public-private partnership and government"

Harpreet Mann
President
Amynta Trade Credit & Political Risk Solutions

Why build a cyber resilience strategy?

To security leaders the drivers for cyber resilience may be obvious: shorter and fewer downtime incidents, reductions in successful attacks, and faster overall resolution, to name a few considerations. But, cyber resilience also has other meaningful business-level impacts, for example helping the organization to simultaneously preserve value while positioning it to generate a sustained return on cybersecurity investments. In an ever-evolving digital landscape, cyber resilience is becoming a key enabler for organizations to stay agile, prepared, and capable of navigating the complex challenges posed by cyber threats. It empowers the C-suite to not just react to incidents, but to proactively shape their organization's cybersecurity posture and protect their digital assets effectively.

Risk management

Risk management continues to be a crucial framing for cybersecurity. State-of-the-art cyber risk management recognizes the critical importance of robust processes, policies, and information systems that consolidate all relevant information and allow for prioritization and continuous response. Such enterprise-wide systems serve as the foundation for effective risk assessment and mitigation strategies. As MunichRe aptly puts it "cyber risk management is core in a digitized world[x]".

Modern cyber risk management requires the aggregation and centralization of all pertinent information related to an organization's cybersecurity posture. This includes data on assets, vulnerabilities, threats, and security controls. Consolidating this information into a single system streamlines risk analysis and decision-making processes.

In our research, and as a recent McKinsey report[xi] details, we see that more organizations are moving away from maturity models to a risk-based approach [xii]. Risk-based approaches align cyber risk management with an organization's risk tolerance and business objectives.

One key component of this approach is the use of key risk indicators (KRIs), which play a pivotal role in providing a consistent evaluation of cyber risks across an organization's assets. KRIs are specific metrics and measurements that help organizations gauge their level of cyber risk. These metrics are selected based on their relevance to an organization's unique threat landscape and objectives. As NIST's report "Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management" notes, KRIs should provide insights into the likelihood and potential impact of cyber incidents and generate a standardized way to evaluate and quantify cyber risks[xiii].

Done properly, KRIs allow organizations to compare and prioritize risks across different assets and systems. This consistency is crucial for making informed decisions about where to allocate resources and prioritize cybersecurity efforts. By assessing risks based on KRIs and tailoring controls accordingly, organizations can optimize their cybersecurity investments and focus resources on areas where they are most needed.

Crown jewels

No matter the approach, all organizations need to tailor their risk management. After all, not all assets within an organization have the same level of importance or face the same level of threat. A key benefit of using KRIs is that they enable organizations to tailor their cyber risk controls to the specific needs of each asset. High-value assets – your organization's crown jewels – or those assets that may be exposed to elevated threats should receive more robust protection measures, while lower-value assets may have more cost-effective controls applied. In our research, we see many organizations still struggle with identification of their crown jewels and would benefit from adopting a trusted methodology to achieve the necessary visibility and prioritization[xiv].

Risk management strategies also should be written using plain language for leaders and practitioners alike. Ditching jargon may be challenging in cybersecurity, but our research shows how impactful plain language can be for resilience. As organizations seek to craft risk management strategies, leaders should bear in mind a recent report detailing the recommendations from the International Standards Association on plain language and its benefits to all industries and sectors[xv].

Minimize financial loss

Cyber attacks can result in substantial financial losses due to data breaches, system downtime, legal costs and penalties, as well as significant reputational damage. Verizon's 2023 Data Breach Investigations Report (DBIR) notes that the financial impact of data breaches is increasing: the average cost of a data breach is now $4.24 million, up from $3.86 million in 2021, with ransomware accounting for one out of every four breaches[xvi].

Cyber resilience measures help minimize these losses by reducing both the likelihood and impact of attacks. In our research, we see that considerations for organizations should include investments in cybersecurity that will enhance your organization's reputation and build trust with partners and clients, the need to meet and even exceed regulatory requirements, and achieving a competitive advantage through cyber resilience.

Enhanced reputation and trust

Organizations that demonstrate strong cyber resilience earn the trust of their customers, partners, and stakeholders. By protecting sensitive data and ensuring business resilience and continuity, organizations can maintain their reputations and competitive advantage. Our research indicates that the ROI for cyber resilience strategies can be as high as 5 to 1.[xvii]

Remember, too, that consumers are also negatively affected by cyber attacks. Allianz and Norton research predict increased attacks against stores of consumer data [xviii]. The Colonial Pipeline hack resulted in gas shortages across the Southeast of the United States. Likewise, attacks against healthcare systems have created chaos for hospitals and patients alike around the world.

As a joint Forbes and IBM report wisely notes: Winning back trust also has a profound cost[xix]. Consumer confidence is a clear differentiator for business. Digital trust is defined by ISACA as "the confidence in the relationship and transactions among providers and consumers within the digital ecosystem[xx]. This includes the ability of people, organizations, process and technology to create and maintain a trustworthy digital world." A 2023 report from IBM also notes that organizations can save an average of $2.66 million by testing their cybersecurity incident response plans[xxi].

> *For my clients who are on the forefront of compliance with what I consider the European gold standard for international global business, they find that their compliance spend – the dollars that they invest in compliance – return a significant investment."*

Linda V. Priebe JD, CIPP/E
Partner, EU-US Data Privacy/Protection & Government Relations, Practus LLP

Regulatory compliance

In many industries and sectors, measures of cyber resilience are closely tied to regulatory compliance requirements. In public and private enterprise, class action lawsuits are significant drivers of change

Over the period of 2022-2023, settlements in data breach class actions or government regulatory actions post breaches have reached into the hundreds of millions of dollars:

Breach or Violation	Settlement/Fine (Millions USD)
Solarwinds[xxii]	26 (to date)
Equifax[xxiii]	575
Meta[xxiv]	277
Capital One[xxv]	190
Morgan Stanley[xxvi]	120

Along with a matured understanding of the role of government to improve transparency and guidance for organizations, stakeholders, and consumers, these class action lawsuits or fines have led to a radically transformed regulatory environment.

For example, consider the changes coming into play with the SEC's cybersecurity rules or the California Consumer Privacy Act (CCPA) where the trends are clearly shifting towards greater transparency and expectations for better security across the board.

By setting clear standards and guidelines, new regulations aim to foster a culture of accountability and best practices which, it is hoped, will ultimately lead to increased resilience against cyber threats. Moreover, these changes are facilitating international cooperation and information sharing, enabling what may become a more unified and collaborative approach to combating cybercrime across borders.[xxviii] As a result, individuals, businesses, and governments are apt to benefit from a safer and more secure digital ecosystem, where innovation can flourish with the confidence that cybersecurity isn't a secondary consideration.

Competitive advantage

In a digital landscape where cyber threats are pervasive and constant, our research suggests that organizations that prioritize cyber resilience are set to gain a competitive edge. Customers, investors, and partners are more likely to choose organizations that demonstrate a robust cybersecurity posture and the ability to withstand cyber attacks.

Gartner predicts that by 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents.[xxix] The same research also predicts that by 2027, 50% of large enterprise CISOs will adopt human-centric security design practices. Achieving cyber resilience goals allows your organization to gain and retain cyber talent in today's highly competitive marketplace.

Time

Remember Benjamin Franklin's adage on the merits of fire awareness and prevention: **"An ounce of prevention is worth a pound of cure."**

More pointedly, downtime costs may not be survivable for many organizations, particularly small to medium-sized enterprises where competition is fierce. In 2022 more than 60% of outages ended up costing businesses more than $100,000. Even worse: 15% cost over $1 million.[xxx]

Time is a critical factor that can greatly influence the impact of cybersecurity incidents on organizations. The cost of preventing a breach, through investments in robust security measures and proactive strategies, is significantly lower than the potentially devastating costs associated with recovering from a breach, including financial losses, reputation damage, legal consequences, and operational disruptions.

Quick incident response is also a linchpin in mitigating the damages caused by a breach. The ability to rapidly detect, analyze, and mitigate threats can significantly reduce the "dwell time" of attackers within an organization's systems, limiting their ability to maneuver and cause harm. This not only minimizes financial losses but also helps prevent the theft or exposure of sensitive data, which can have far-reaching consequences for both individuals and the organization as a whole.

Time can work both for and against organizations. The costs of preventing a breach is far smaller than that of recovering from a breach. Research indicates the one surefire method of reducing the costs of a breach is faster incident response. Given the pressing challenges, cyber resilience allows CISOs not only to react but to shift to a strategic proactive approach.

> *By the time there's an adverse security incident they're usually in your systems. They've already been able to exfiltrate data and do damage and they may have been in there for years. We really need to be focusing on making sure we do cyber right the first time."*

Mary Frantz
Managing Partner
Enterprise Knowledge Partners

Integrating a new model for risk management

We have found that many organizations are now commencing with implementation of cyber resilience processes to proactively identify and remediate issues quickly and at scale. Our research indicates that organizations are starting starting by examining the necessary building blocks of people, process, and technology, leading to awareness that cyber resilience requires robust risk management to enhance security. Our survey results indicate that cyber resilience measures include applying best practices in risk management to conform with guidance and recommendations which in turn provides the organization with a solid defense in the event of an attack.

While there are many variations and many frameworks, from Gartner's Continuous Threat and Exposure Management (CTEM) to NISTs Cybersecurity Framework, there is broad alignment in approaches around very similar risk management concepts.

At the heart of all processes and frameworks for cyber resilience (including this one from Red Sift) is that the process must be situated in risk management. With risk management policies in place, we can know what to do when things go wrong. Risk management done right sheds light on roles, responsibilities, what to protect and at what level, and more.

Critically, it should be understood that cyber resilience is a continuous cycle – again, there's no such thing as "one and done." Instead, a resilient organization is constantly evolving to meet changing risks and needs. Done properly, the cyber resilience process outlined below will be nimble while continuously working stepwise, based on organizational bandwidth and emerging threats.

We also note that increasingly large, cumbersome cross-departmental initiatives are being broken into multiple, parallel agile projects. (Remember that time is the new currency.) As such, our approach is broken down into five steps: **Focus, Action Plan, Verify, Prioritize,** and **Discover**.

> *Cyber resilience is the cornerstone for trust in the digital world. It enables a secure supply chain and the flow of data. It gives organizations the ability to truly safeguard their stakeholders and customers while demonstrating commitment to the future."*

Helio Cabral Santana
Cybersecurity Operations Change Managemen
Forvia

1 2 3 4 5

A five step process for resilience

Step 1: Focus

The death of any strategic initiative is trying to do everything at once. According to recent studies, some 60–90% of strategic plans never fully launch. And that is no different in cybersecurity.[xxxi]

As Amadeus Mozart once said, "the shorter way to do many things is to do one thing at a time." That same principle of sequencing applies in cybersecurity: many security and risk frameworks fail to properly take sequencing into account, forcing organizations to start with the step of gathering mountains of data and intelligence about all potential exposures, risks, and threats the organization has or could face. z

And yet the reality, as ISSA's 2023 Life and Times of a Cybersecurity Professional report details, is that today's cybersecurity teams are almost universally understaffed and tasked with supporting and sustaining the organization against constant challenges.[xxxii] ISSA notes that for a majority (63% of those surveyed) of those working cybersecurity, they feel their work has become more difficult over the past two years. For most, understanding the overall cyber risk is bound to lead to large backlogs of items that may never be actioned. Instead, CISOs or others charged with managing cyber risk should begin by scoping the current iteration of the cyber resilience process.

Our process can be scoped on:

- **an attack surface**
  (ie., external-facing assets, cloud assets)
- **by threat vector**
  (ie., lookalike domains, insecure emails),
- **by business application**
  (ie., brand abuse, executive impersonation).

Critically, you need to start somewhere and build out.

Step 2: Action plan

While many cybersecurity approaches make the last step "fix" or "recover," the action plan for remediation is best considered shortly after a project is scoped.

This can be helpful for scenario planning, identifying key stakeholders to involve in the process, and gaining organizational alignment on resources and timeline.

For example, if a current cyber resilience initiative is focused on brand abuse, security teams should not wait until impersonating websites are discovered to create a plan for resolution. Instead, the cross-functional team should agree on the action that will be taken when an impersonating website is discovered.

It is imperative to begin with the end in mind and build the plan accordingly.

Digital transformation has made this step even more important than it once was. While there are often automated fixes for issues - like patches or upgrades – it is becoming increasingly common for remediation to require human intervention. All the while the non-patchable surface is growing. Gartner estimates that today 10% of the enterprise's total exposure is not patchable. But by 2026, that number is expected to increase to 50%, dramatically reducing the impact of automated remediation practices.

Action plans will require the involvement of non-technical stakeholders as well. This should include employee training, business-wide communications about new threats, and regular conversations with the board and C-suite about enterprise-level risk.

Going forward, action planning will be centered upon leadership's ability to drive organizational change when critical challenges are discovered.

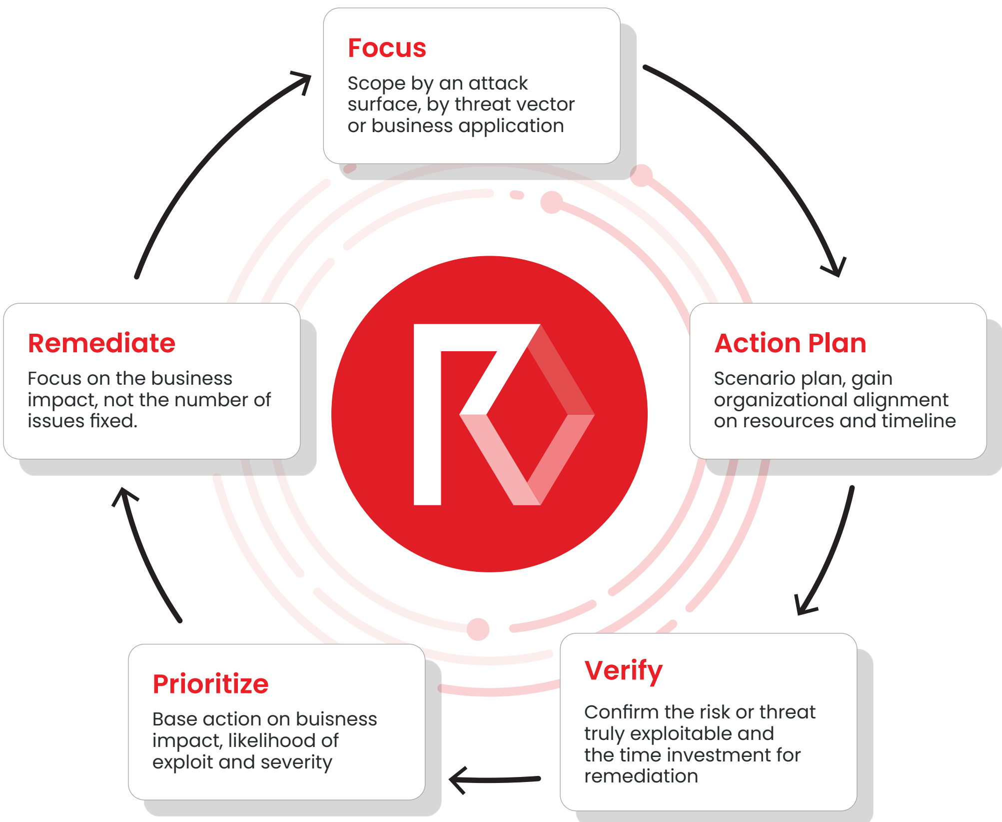
Step 3: Verify

Once a team has scoped this iteration of the cyber resilience process and worked cross-functionally to agree on an action plan with stakeholders, they need to verify that remediating the identified exposures, risks or threats is the best investment of resources – including time.

Generally, this comes down to three key questions:

- **Is this genuinely exploitable? 85 percent of security issues in backlogs cannot be exploited.**[xxxiii]
- **What are the attack paths? And which are most likely to be exploited?**
- **Can we remediate it quickly enough to have an impact?**

The best way to do this is to see your organization through the eyes of an attacker. Once dominated by larger organizations, the “attacker’s eye view” approach is becoming widely accepted and is the key to having an anticipatory strategy. Shutting open doors and hardening your defense is critical to making yourself less likely to suffer a costly breach.



Step 4: Prioritize

Once issues have been validated as truly being exploitable, the security team can then begin prioritizing the issues to be fixed.

In short: Risks that are in scope and have been validated as truly exploitable should be prioritized based on business impact, likelihood of exploit and severity.

While automated tooling can be helpful in classifying risks with traffic light systems, or 'high', 'medium' and 'low' classifications, human intervention taking full advantage of people, process, and technology is required to truly prioritize what is most important to protect critical assets.

Step 5: Remediate

Automated tools are critical to achieve remediation at scale. Critically, it is important that the discovery technology used is suitable for the scope.

Remediating risks does not begin and end with patching critical vulnerabilities. Instead, the security team and those charged with enterprise risk management need to take a holistic view of accounting for known and unknown risks. These might be lookalike assets, vulnerabilities, misconfiguration and any other doors that could be opened by bad actors.

The key to this step is realizing the number of issues is not the metric to optimize. The key is the business impact the team can have (and communicate about effectively). Remember, this is about plain business language. The moment you go off in the direction of extensive technical complexity, you will lose a considerable portion of your stakeholders' and leadership's attention and, worse, run the risk of losing critical buy-in when you need it most.

Changing cultures of risk awareness

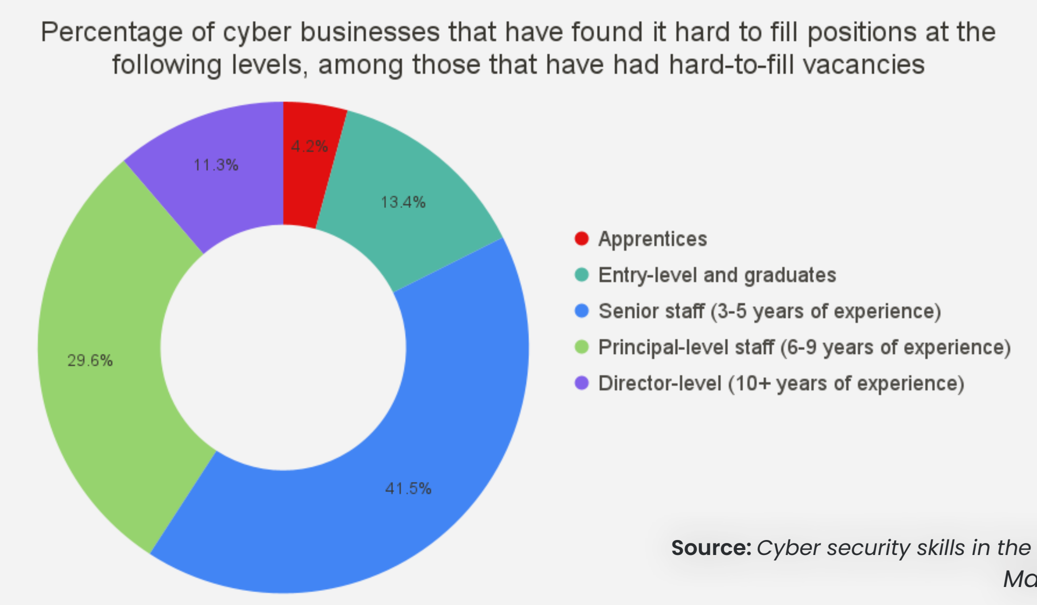
Critical components of cyber resilience

As with nearly every security initiative, pursuing a cyber resilience strategy cannot happen in a silo. Even with the right documented process in place, C-suite leaders need to also leverage people and tools effectively for the initiative to succeed.

People

Human factors in cybersecurity encompass the intricate interplay between human behavior, psychology, and the technological systems that underpin cybersecurity. Understanding and addressing these factors is essential because humans are both the users of technology and potential points of vulnerability. Moreover, human factors extend to the design of user interfaces and systems, where usability and user-centered design directly influence the adoption of secure practices.

It is widely accepted that humans are often the weakest link in any security strategy. As noted earlier in this report, by one measure some 74% of all corporate data breaches involved people making mistakes. For a cyber resilience program to succeed, it needs to also include robust cybersecurity policies and employee training. But training alone only gets you so far and can become the basis of a blame culture.



Source: *Cyber security skills in the UK Labour Market, 2023*

> *Security culture is the foundation for organizational resilience against security threats [...] when it comes to managing human-centric security risk, organizations need to move beyond compliance-based interventions and design solutions that mitigate the drivers of the behavior causing the risk."*

Owen Pierce
Associate Director
Management Consulting Transformation Group, KPMG

The shortage of skilled cybersecurity professionals continues to be a challenge globally. According to the World Economic Forum, the world needs 3.4 million cybersecurity experts[xxxiv] to support today's global economy, but the industry is struggling to fill that gap.

Organizations are competing for a limited pool of experts who can effectively design, implement, and manage robust cybersecurity strategies. Yet, the demand for cyber security professionals continues to increase. The United Kingdom's report[xxxv] on the "Cyber security skills in the UK labour market 2023" noted that the average number of vacancies per firm has gone up from 6.8 in the 2022 report to 8.2 this year. And firms are finding it harder to fill vacancies.

Culture

Anticipating, adapting to and overcoming breaches requires cultural shifts in how businesses manage risk. As happened with the shift to DevOps, our conversations around incidents need to be modeled on "just culture.[xxxvi]"

In 2023 the term "cyber shame" was selected word of the year by Cyberspace Netherlands and the Cyber Alliance for their cybersecurity dictionary.[xxxvii] In keeping with our research, we have found that the organizations involved understand that – given the mounting pressures –there simply is no space for blame culture. Starting with blame-orientated questions in training will make things worse and cause people – your most important asset – to ignore or avoid potential security issues. It's better to strengthen your organization's security culture through shame-free training and awareness, ultimately addressing root causes as the most effective way to build a cyber resilient culture.

Remember. You want your staff and leadership to flag potential problems. If they can see an issue, it's likely your adversaries can as well.

Communication & collaboration

Effective communication within an organization and with external stakeholders is crucial before, during, and after a cyber incident. Organizations need to be primed to think about and plan for communications with multiple stakeholders, often involving both public and private sectors, to improve cyber resilience. Promptly and transparently notifying relevant parties, such as customers, partners, and regulatory bodies, builds trust and allows for coordinated efforts to mitigate the impact of attacks..

Understanding the steps of building a cyber resilient organization is key for CISOs, and it must be communicated as a high-level strategy for board conversations. This should be done proactively and on a regular cadence to keep the conversation from focusing exclusively on current risks and threats.

In all presentations, security leaders should remind the board that security is not a “fix and forget” endeavor but a living and ongoing effort. Cyber resilience is a continuous process that adapts to the realities of a given business in as close to real time as possible. CISOs must translate technical findings and plans into risk management conversations and may choose the following approach:

CISO risk management

1. **An assessment of the current risk position** informed by the scoping and discovery phases of the cyber resilience process.
2. **A prioritized list of actions (current and future)** through a risk management lens. Leverage your findings from the prioritization and validation and communicate the business-level impact of potential impacts. Instead of focusing on the technical issues, like the number and severity of lookalike domains that the team discovered, focus on the message of protecting your business from brand abuse, impersonation and fraud.
3. **A go-forward strategy** using your findings from the mobilize phase, include a summary of the actions and outcomes your team has delivered since your last update and plans for what’s next. When possible, tie this into business-level metrics including incidence rates, severity levels, response times, and mean time to remediation with trends over time.

Take the positive example of Werner Lanthaler who rushed to the office after learning his biotech company Evotec had been hacked. In what may become an example for other CEOs to follow, according to the Wall Street Journal Lanthaler took an “uncommonly active, public role in the cyber response at Evotec. He communicated personally with business partners, wrote an open letter about the attack in the midst of Evotec’s ordeal and held town-hall meetings with employees every few days to provide updates.[xxxviii]

Our research suggests that organizations that think of communication as a form of collaboration are able to use communications as a potent catalyst for bolstering cyber resilience across their digital landscape. By uniting diverse expertise, resources, and perspectives, collaborative efforts amplify the collective ability to anticipate, respond to, and recover from cyber threats.

ENISA's 2023 AR in Box Report offers a method to follow for organizational cyber awareness.[xxxix]

The core elements can be distilled into the following key points:

- **Deliver the right message to the right employee group.**
- **Understand that message formulation is critical for success.**
- **Select the appropriate tools to generate awareness..**
- **Learn by monitoring and evaluating.**

The effects of such collaboration are far-reaching, leading to the rapid dissemination of threat intelligence, best practices for incident response, the cultivation of cross-sector partnerships, and the development or maintenance of trust. As organizations and nations share insights and experiences, a dynamic cycle of learning and improvement emerges. This not only strengthens individual defenses but also fosters a cohesive global defense network that transcends geographical boundaries.

Enabling technologies

"Complexity has become the bane of security and simplicity is the arch nemesis of our adversaries. So, we want things to be secure by design & secure by default out of the box."

Gregory Touhill
Director, Carnegie Mellon University Software Engineering Institute's CERT Division

New technologies are playing an instrumental role in enhancing cyber resilience for organizations in today's digital landscape. Advanced threat detection and mitigation tools, increasingly powered by artificial intelligence[xl] and machine learning algorithms, enable real-time monitoring of network traffic and ever-more rapid identification of suspicious activities or anomalies.[xli] Additionally, technologies are revolutionizing data integrity and authentication, reducing the risk of data tampering and unauthorized access. Cloud-based disaster recovery solutions are providing scalable and cost-effective ways to ensure business continuity in the event of cyberattacks or system failures. Furthermore, automation and orchestration tools are streamlining incident response, enabling organizations to react swiftly to threats and minimize potential damage.

By embracing these innovative technologies, organizations are becoming better equipped to proactively defend against cyber threats and recover swiftly when incidents occur, ultimately bolstering their overall cyber resilience.

Tools

Prevention

Looking through the eyes of an attacker and taking proactive measures to harden any weaknesses an attacker would see is acknowledged as the best way forward to significantly reduce the likelihood of a successful cyber breach.

At base, standard preventive measures should include protection against:

- **Exact domain impersonation**
- **Lookalike domain impersonation**
- **Logo brand abuse**
- **Expiring, mis-issued, and misconfigured certificates**
- **Open ports**
- **Poorly configured DNS and dangling DNS issues**
- **Incorrect usage of the domain, email, and web standards available that when used properly will protect against common PKI, TLS, HTTP and browser attacks.**
- **Usage of HTTP not HTTPS**

Our research indicates that the appetite of attackers to take advantage of these weaknesses simply never reduces.

- **Recent research by Certitude Consulting demonstrated how simple it can be for attackers to identify assets that can be at risk of takeover because of dangling DNS.[xlii][xliii]**
- **Every organization has problems because of misconfigured and expiring certificates. Shopify, Microsoft, Spotify, Starlink[xliv], Bank of Ireland, and Twitter have all recently had high=profile issues.**
- **Google is proposing a 90-day certificate lifecycle. Its intention is to encourage automation. But it will also increase the volume of certificates within an estate, and therefore the attack surface.**
- **Cloud asset misconfigurations accounted for 19% of compromise factors in Google Cloud incidents reported by customers.[xlv]**

By implementing strong preventive measures, organizations can significantly reduce the likelihood of successful cyber breaches.

Detection and response

Despite preventive measures, cyber incidents can still occur. As former FBI Director Robert Mueller succinctly put it at RSA in 2012: "it is no longer a question of 'if' but 'when' and 'how often'. I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again[xlvi]."

Given the risks, organizations should work in earnest to establish risk management plans and invest in advanced threat detection systems. To that end, we recommend that the following capacities should be included in an advanced detection system:

- **Domain threat intelligence**
- **Digital brand protection**
- **Certificate transparency monitoring**
- **Certificate lifecycle management**
- **Vulnerability management**
- **Asset configuration monitoring - can be part of attack surface monitoring**
- **Cloud security posture management**
- **Web application firewalls**

> *The first step to mitigate cyber risk and enable resilience is achieved through awareness. It's about visibility - you can't control what you can't see."*

Michal Wojnar
Cyber Security Director, Cyber & Privacy
PwC CZ/CEE

Mapping GRC in 2023

The landscape of Governance, Risk, and Compliance (GRC) is undergoing a profound transformation to meet the growing challenges to cyber resilience. Traditionally, GRC has been primarily focused on regulatory compliance and risk management, but that work has often taken place in silos. Our research suggests that many organizations' efforts remain fragmented, reflecting the complex compliance ecosystem, and often that results in an incohesive global strategy. However, we also see that in the context of cybersecurity, the paradigm is shifting towards a more integrated and proactive approach.

Modern GRC frameworks are now designed to incorporate cyber risk management as a core component, aligning it closely with an organization's overall business strategy. This shift recognizes that cyber resilience is not just about meeting compliance requirements but involves actively identifying, assessing, and mitigating cyber risks. Integrated GRC platforms also leverage data analytics and automation to provide real-time visibility into an organization's cyber risk posture, enabling more agile responses to emerging threats. Additionally, such systems promote collaboration and communication across various departments, breaking down the silos that often hinder an effective response to cyber incidents.

In 2023, the regulatory landscape in the realm of cybersecurity has undergone a significant transformation, with several key frameworks and bodies that we detail below playing pivotal roles. The U.S. Securities and Exchange Commission (SEC) has intensified its focus on cybersecurity disclosures, obliging companies to provide more comprehensive insights into their cyber risk management. The Digital Operational Resilience Act is in force and has already been instrumental in promoting transparency and accountability. The National Institute of Standards and Technology (NIST) continues to lead the charge in setting cybersecurity standards and guidelines, adapting to the evolving threat landscape. The Payment Card Industry (PCI) Security Standards Council has expanded its efforts to enhance payment card data security. Meanwhile, the European Union Agency for Cybersecurity (ENISA) has taken strides in fostering cyber resilience and cooperation across Europe. These developments underscore the growing importance of regulatory compliance and cyber resilience in an era where digital security is paramount.

“Well-informed board members bring us one step closer to corporate stability and enterprise-wide resilience in the face of complex and continuing adverse cyber incidents.”

Annie Searle
Principle
Annie Searle and Associates

Often established by governmental bodies with detailed input from industry or by industry coalitions, these developments serve as frameworks that may mandate specific security protocols, data protection measures, and incident response plans. Meanwhile, this standardization brings a level of consistency and rigor to cybersecurity practices across sectors, facilitating a collaborative defense strategy that benefits not just individual organizations, but the industry and public at large.

New legal obligations often assume a multi-jurisdictional element as conformance to standards is becoming essential for firms globally, particularly those that access the EU market. By aligning and adhering to frameworks and regulations, organizations not only mitigate the risk of cyberattacks but also improve their market reach as well as the capacity to recover and adapt when breaches do occur.

Moreover, regulations help to ensure that companies invest adequately in cybersecurity infrastructure and personnel, elevating the importance of digital security to a boardroom priority. All of which makes cyberspace more resilient in an increasingly complex and volatile landscape. The good news is that the changes in frameworks and regulations are fully aligned with known, enterprise-wide risks.

Bottom line up front: Inadequate security processes or not knowing or reporting on problems will no longer serve as excuses.

In essence, the changing face of GRC is all about ensuring that cyber resilience becomes an integral part of an organization’s DNA, fostering a proactive, adaptive, and holistic approach to cybersecurity.

SEC cybersecurity rules

In the United States, one of the key drivers for positive change in cyber resilience is the updated cybersecurity rules from the Securities and Exchange Commission[xlvii]. The rules aim to enhance the resilience of publicly traded companies against cyberattacks and to improve the protection of sensitive customer information and market integrity.

The SEC’s moves were prompted by escalating and sophisticated cyber threats, negative impacts on investors and stakeholders (to include market disruptions that can affect investment decisions and undermine trust in the financial system) and regulatory gaps that necessitated new rules to address emerging threats and enterprise-wide operational challenges.

The new disclosure requirements[xlviii] for companies related to cybersecurity incidents and risk management are set to take effect on September 5th 2023, with disclosures on risk and governance to be made in annual reports for fiscal years that end on or after December 15th, 2023.

For all publicly traded companies there is a new rule for reporting material cybersecurity incidents in four days – that means that companies will have to know their assets and continuously monitor their risks. Violations will be a range and are growing progressively larger, e.g. Pearson was fined $3 million USD for allegedly misleading cyberattack disclosures.[xlix] Key points of these requirement include:

Material cybersecurity incidents disclosure

- Companies must disclose any material cybersecurity incident, detailing its nature, scope, timing, and potential impact. A Form 8-K, Item 1.05 must be filed within four business days after determining the incident's materiality.
- Immediate disclosure can be delayed by the U.S. attorney general in cases of substantial national security or public safety risk.
- Companies must later amend their initial filings to include previously unavailable incident information.
- Foreign private issuers will use Form 6-K to report material cyber incidents disclosed outside the U.S.[l]

Risk management and strategy

- Companies are required to describe their approach to managing cyber threats, including assessment and identification procedures.
- They should disclose whether cyber threats have materially affected or are reasonably likely to affect finances, operations, or business strategy, under Regulation S-K Item 106(b).
- Governance details include the board's oversight of cyber threat risks and management's handling of material cyber risks.

Enforcement timeline

- Governance and risk management disclosures must be made in annual reports for fiscal years ending on or after December 15 2023.
- Incident disclosure requirements must be met starting from December 18.
- Smaller companies have until June 15, 2024, to comply with the incident disclosure requirements.

Materiality determination

- Companies must focus on disclosing incidents material to their business rather than adhering to rigid rules.
- Materiality can be determined by considering quantitative and qualitative outcomes.
- Incidents affecting a company's reputation, customer relationships, vendor interactions, and competitive ability can be considered material.[li]
- Materiality is established based on what a "reasonable investor" would find significant for the company.
- The SEC received feedback regarding materiality and timing, with suggestions to extend disclosure timelines or set tangible triggers for materiality determination.

Remember: a material cybersecurity incident is typically defined as an incident that: (1) has a significant impact on the company's ability to provide products or services; (2) results in the unauthorized access, use, disclosure, or loss of material nonpublic information; or (3) otherwise has a significant negative impact on the company's financial results, operations, or reputation.

Overall, these new rules compel companies to disclose material cybersecurity incidents and offer some detail about their risk management strategies. The SEC continues to emphasize a flexible approach, urging companies to focus on what would matter to investors and customers rather than adhering to strict criteria. The SEC'S approach aims to enhance transparency and readiness in the face of increasing and cascading cyber threats.

Digital Operational Resilience Act

In 2008 as the global financial crisis started to bite, countries, companies, and communities learned how interconnected the financial sector was. Later, to guard against a similar crisis, measures were introduced to strengthen the financial resilience of the financial sector.

Overlooked at that time was the digital operational resilience of those same entities. Increasing digitalization and consumers' reliance on digitalization as well as the interconnectedness of the financial sector itself has amplified Information and Communication Technology (ICT) risks.

Previous efforts to address these gaps led to overlaps, inconsistencies and a duplication of requirements at national and European Union level increased complexities and costs. Ultimately, the absence of a single cohesive response undermined the stability and integrity of the European Union financial sector whilst also increasing the costs for businesses in this sector.

By establishing a comprehensive framework, the Act seeks to protect consumers and investors, enhance financial stability, reduce costs and support the competitiveness of the EU financial sector.

To achieve these aims, the act sets out specific requirements across six pillars:

- **Governance**
- **ICT risk management**
- **ICT incident reporting**
- **Digital operational resilience testing**
- **ICT third-party risk management**
- **Information and intelligence sharing**

DORA focuses on Information Communication Technology (ICT) risk management requirements and sets out key principles for identifying, protecting, detecting, responding, and recovering from ICT risks. The Act itself is not unduly burdensome as it builds upon existing cybersecurity frameworks and international standards.[lii] This approach ensures harmonization with established best practices, minimizing the deviations for financial entities that have benchmarked them. This reduces complexity and therefore reduces the cost to comply.. The introduction of specific Governance obligations was unprecedented but welcomed. In particular the requirement for the management body to follow specific training to 'gain and keep up to date sufficient knowledge' was in all probability as a result of information asymmetry challenges faced by CISOs and CIOs trying to access budget for essential solutions.

DORA emphasizes the need for resilient ICT systems and tools, continuous monitoring of ICT risks, prompt detection of anomalies, establishment of business continuity policies and disaster recovery plans, and learning from both external events and ICT incidents.

NIST Cybersecurity Framework 2.0: now with "Govern"[liii]

The National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) is a voluntary set of guidelines designed to help organizations improve their cybersecurity posture and overall resilience.

Familiar to all in cybersecurity and in use around the world, the NIST CSF was originally organized around five core functions: **Identify, Protect, Detect, Respond, and Recover.**

- **"Identify" helps organizations understand their digital assets and the related cybersecurity risks, which is the foundation for any effective cybersecurity strategy.**
- **"Protect" outlines best practices to safeguard these assets and reduce vulnerabilities, thus acting as a preventative measure against cyber threats.**
- **"Detect" emphasizes the development of capabilities that quickly identify cybersecurity incidents. Quick detection is crucial for minimizing damage and for initiating an effective response.**

- **“Respond” provides guidance on taking appropriate actions when a cybersecurity incident occurs, ensuring that the incident is contained and controlled. This involves having a predefined incident response plan and communication strategy.**
- **“Recover” focuses on restoring and validating system functionality for business operations to resume. It also emphasizes learning from past incidents to improve future cybersecurity measures.**
- **And in 2023, after a public comment period a new function was added: Govern. This function focuses on establishing and implementing an effective cybersecurity governance structure within an organization.**

The Govern function involves defining roles, responsibilities, and decision-making processes related to cybersecurity at various levels of the organization, from senior leadership to operational teams.
By incorporating the Govern function, NIST aims to bridge a significant gap between technical cybersecurity measures and the strategic decision-makers and processes within organizations. As with DORA and the SEC’s cybersecurity rules, NIST’s recognition underscores the need for cybersecurity to be an enterprise-level concern, aligned with an organization’s enterprise objectives and risk appetite.

Through its comprehensive yet adaptable structure, the NIST CSF encourages organizations to take a proactive approach to cybersecurity. It allows for customization based on the specific risks and needs of each organization, making it applicable across various industries. By following the NIST CSF, organizations not only improve their defenses against immediate threats but also build a culture of continuous improvement in cybersecurity, thereby enhancing their resilience in the long run. We find that this holistic and systematic approach should allow organizations to assess their current cybersecurity capabilities, set goals for cybersecurity measures, and implement practices that help in resilience.

EU Cyber Resilience Act

The EU’s proposed Cyber Resilience Act[liv] signifies a robust step forward in the realm of cybersecurity regulations, aiming to fortify the security standards for products with digital components.

The EU’s regulatory proposal addresses two primary issues that contribute to escalating costs for both users and society at large:

Firstly, the prevalence of cybersecurity vulnerabilities and the inadequate dissemination of security updates have led to a critical deficiency in the cybersecurity of such products. This lack of security not only exposes users to risks but also imposes societal burdens. Secondly, the inadequate comprehension and accessibility of information for users hinder their ability to choose products with adequate cybersecurity attributes and utilize them in a secure manner.

While current EU regulations apply to certain products with digital elements, the majority of hardware and software products remain unregulated in terms of their cybersecurity. This deficiency is especially concerning given the escalating cyber threats that exploit vulnerabilities in these products, resulting in substantial social and economic consequences. The World Bank projects[lv] that 10.5 million records are lost or stolen every month, 438,000 every hour; and that a single large-scale attack can trigger $53 billion in economic losses.

The objectives of the Cyber Resilience Act are twofold: to foster the creation of secure products with digital components by ensuring they enter the market with minimal vulnerabilities and that manufacturers prioritize security across the entire product lifecycle, and to empower users to factor in cybersecurity when selecting and using products with digital components. (In the United States, CISA is also focused on security-by-design and has released a report in 2023 on "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-byDesign and -Default).[lvi] The EU's proposed Cyber Resilience Act outlines four key objectives:

- **Enhancing manufacturer accountability:** Manufacturers will be required to enhance the security of products with digital elements from the outset of design and development, ensuring security remains a priority throughout the product's lifecycle.
- **Establishing a coherent cybersecurity framework:** The act seeks to create a comprehensive cybersecurity framework that simplifies compliance for both hardware and software producers.
- **Increasing transparency of security attributes:** Enhanced transparency will facilitate a better understanding of the security features of products with digital elements, aiding consumers in informed decision-making.
- **Promoting secure use of products:** The act is designed to empower both businesses and consumers to use products with digital components in a secure manner.

By enhancing security standards, transparency, and user awareness, this proposed regulation aims to create a safer digital landscape while also fostering a more resilient and secure digital economy.

PCI DSS 4.0 and cyber resilience: new requirements include DMARC

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. The updated PCI DSS 4.0[lvii] aims to offer a more flexible approach to achieving and demonstrating compliance, as well as addressing the evolving cybersecurity landscape. PCI released version 4.0 of the standard in March 2022. While PCI DSS v3. 2.1 will remain active through March 2024, there will be a year-long transition to PCI DSS 4.0 with full force in March 2025.

A major addition to the PCI DSS is the requirement for DMARC[lviii] which helps organizations to build resilience against a range of email-based cyber threats by providing authentication and reporting mechanisms. This not only limits the success of phishing attacks but also provides organizations with the information they need to continually assess and improve their email security, thereby contributing to an overall more robust cybersecurity framework.

Key features of PCI DSS 4.0

- **Adaptive security model:** PCI DSS 4.0 introduces an adaptive and flexible framework that allows organizations to tailor security controls to their unique environment and risk landscape.
- **Emphasis on security outcomes:** Unlike its prescriptive predecessors, PCI DSS 4.0 focuses on the desired outcomes of security controls, allowing for greater flexibility in how those outcomes are achieved.
- **Enhanced authentication mechanisms:** Advanced multifactor authentication methods are expected to become a more prominent requirement, reducing the likelihood of unauthorized access.
- **Secure software lifecycle:** PCI DSS 4.0 incorporates more explicit requirements around secure software development and the secure handling of software updates

How PCI DSS 4.0 aids in cyber resilience

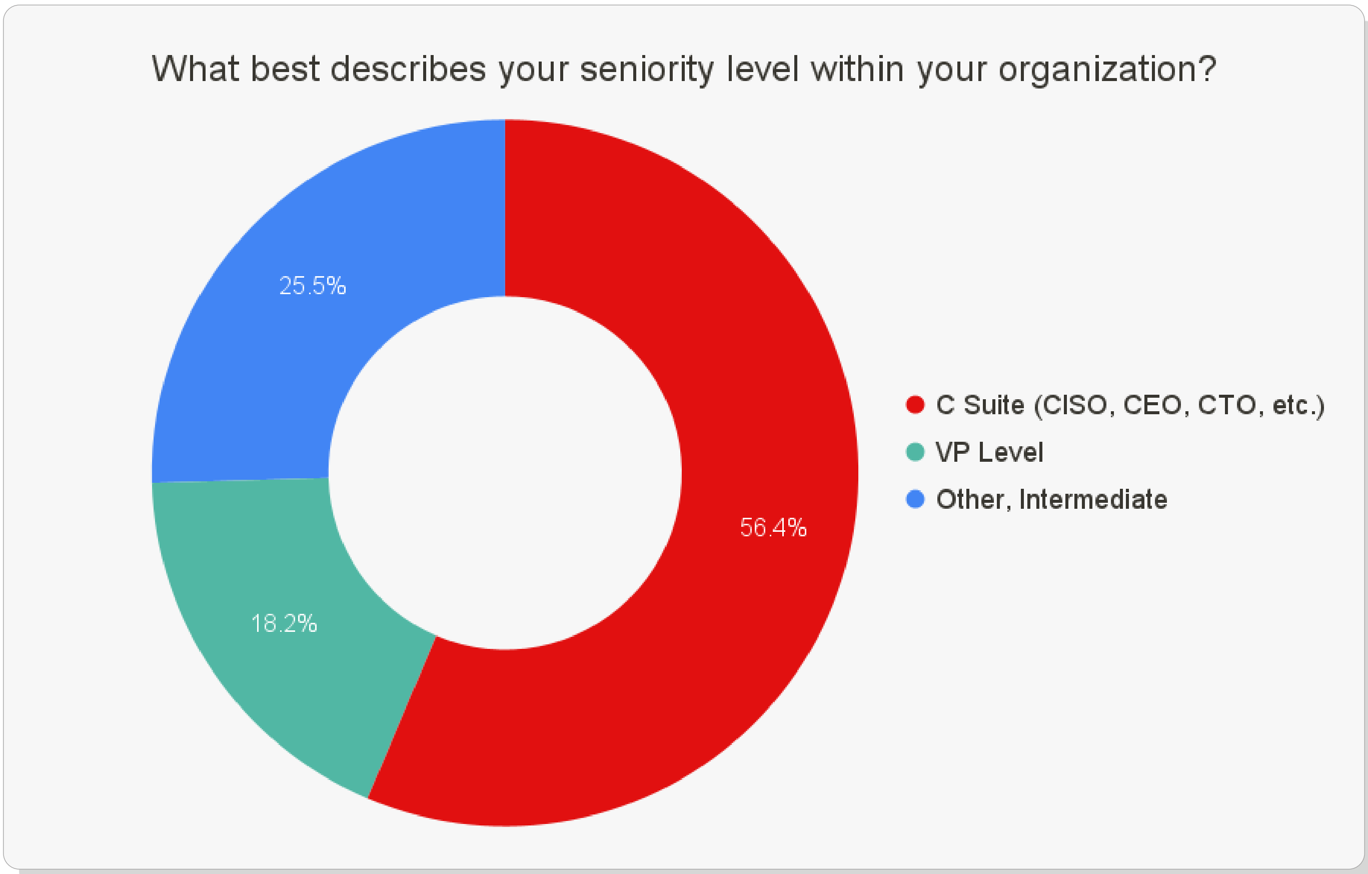
1. **Proactive risk management:** By emphasizing an adaptive security model, PCI DSS 4.0 encourages organizations to actively assess and adapt to risks, thereby enhancing their cyber resilience.
2. **Business continuity:** The focus on outcome-driven security controls means that organizations are better equipped to maintain operations even when they are under cyber threats, aiding in business continuity.
3. **Data protection:** Stronger authentication and encryption measures help in safeguarding sensitive customer information, thus increasing the organization's resilience against data breaches.
4. **Supply chain security:** By extending its requirements to third-party service providers and incorporating secure software development practices, PCI DSS 4.0 helps address vulnerabilities in the supply chain, a significant point of entry for cyber threats.
5. **Enhanced incident response:** One of the anticipated features of PCI DSS 4.0 is an improved framework for incident detection and response, enabling organizations to better prepare for, respond to, and recover from cyber incidents.
6. **Standardization and benchmarking:** PCI DSS 4.0 serves as a benchmark for payment security, enabling organizations to align their security strategies not just for compliance but as a part of a broader cyber resilience strategy.
7. **Visibility and monitoring:** Enhanced requirements for logging and monitoring will allow organizations to have better visibility into their security posture, facilitating faster detection and mitigation of potential security incidents.

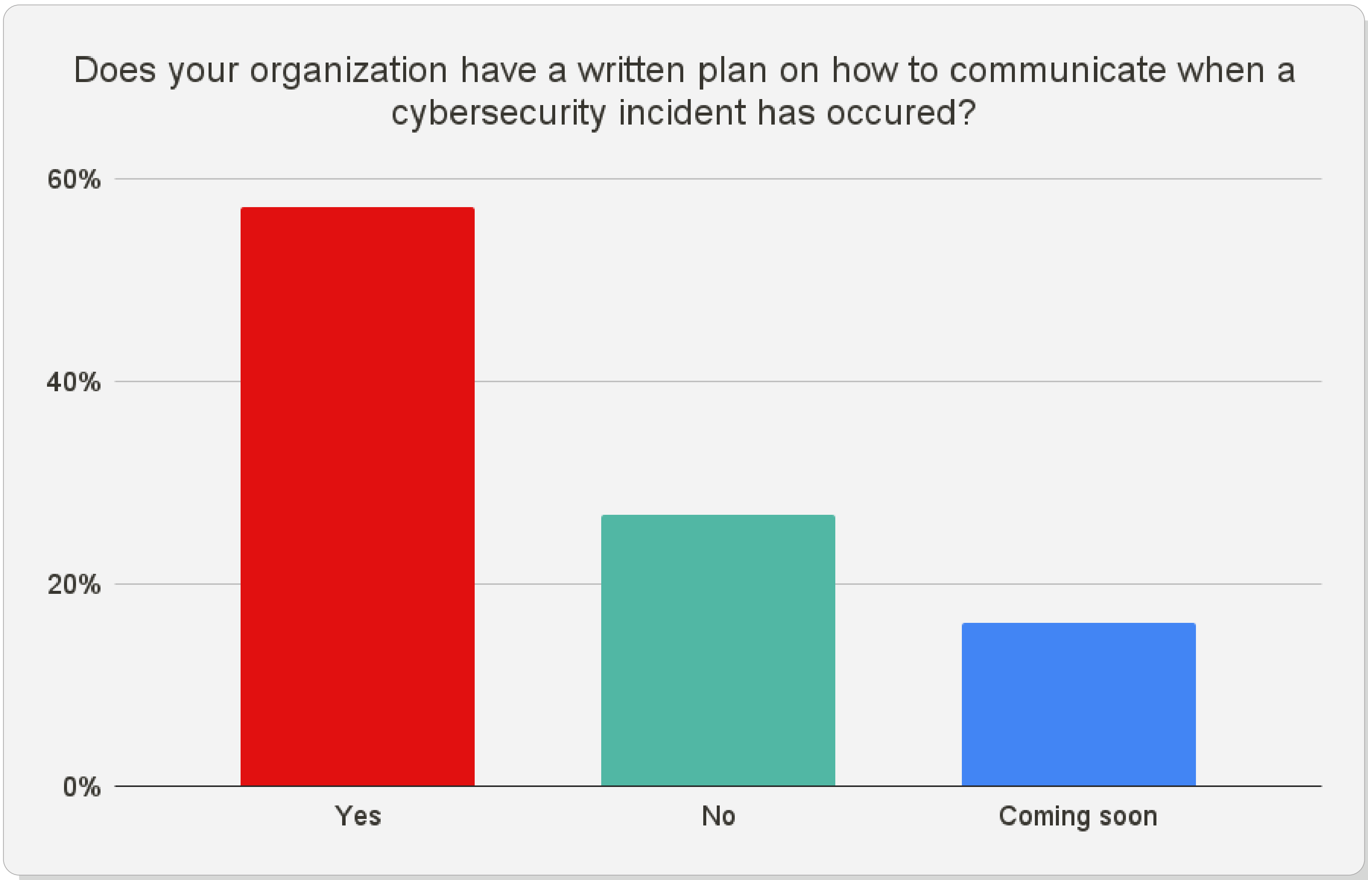
PCI DSS 4.0 will prove to be a more adaptable and outcome-focused standard that not only ensures the secure processing of payment information but also contributes significantly to the cyber resilience of organizations. By incorporating modern security approaches and providing the flexibility for businesses to adapt to their specific needs, it offers a robust framework for organizations to improve their overall cybersecurity posture.

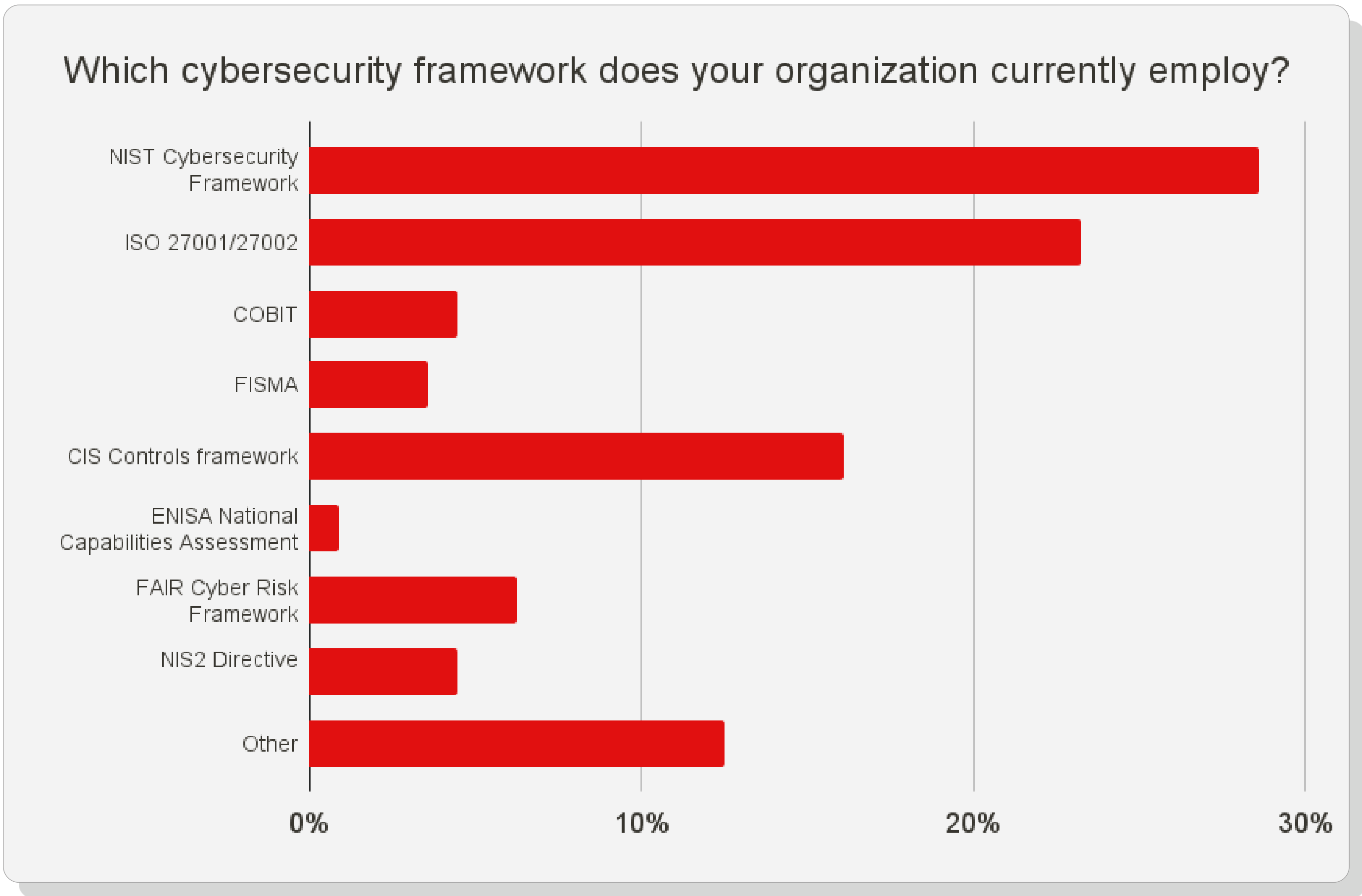
Red Sift Resilience Survey 2023

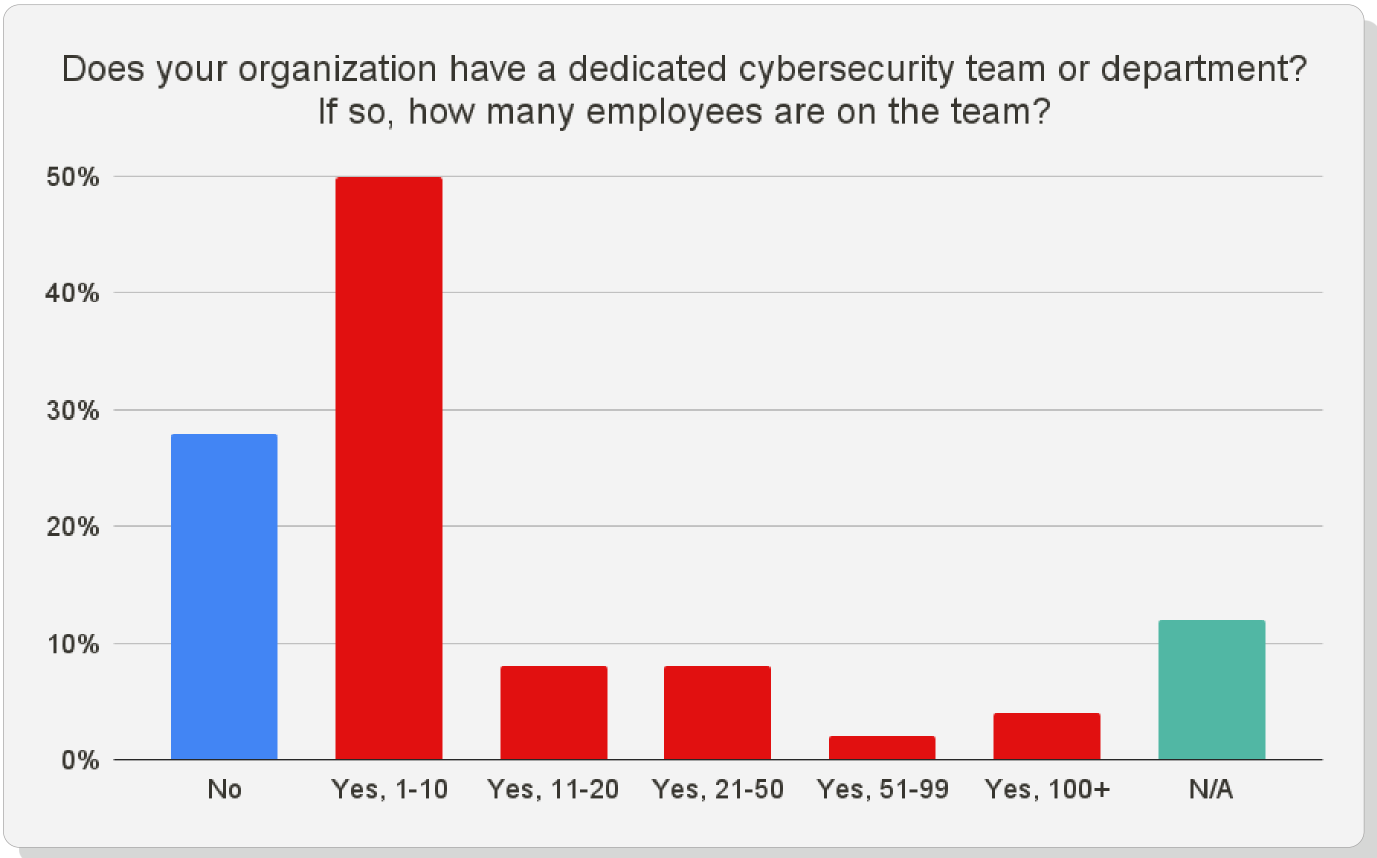
The State of Global Cyber Resilience Survey, distributed to executives across diverse industries, has yielded invaluable insights into the intricate tapestry of cybersecurity practices. The survey delved into a dynamic mix of roles and responsibilities and spending patterns, showcasing how organizations understand and allocate resources to fortify their cyber defenses. This survey was meticulously crafted to ensure its relevance to the challenges faced by organizations today. To ensure a diverse and representative sample, we targeted 60 top cybersecurity and C-suite executives across various industries. These individuals were chosen for their expertise and leadership roles, providing a wealth of experience and insights into the cybersecurity landscape.

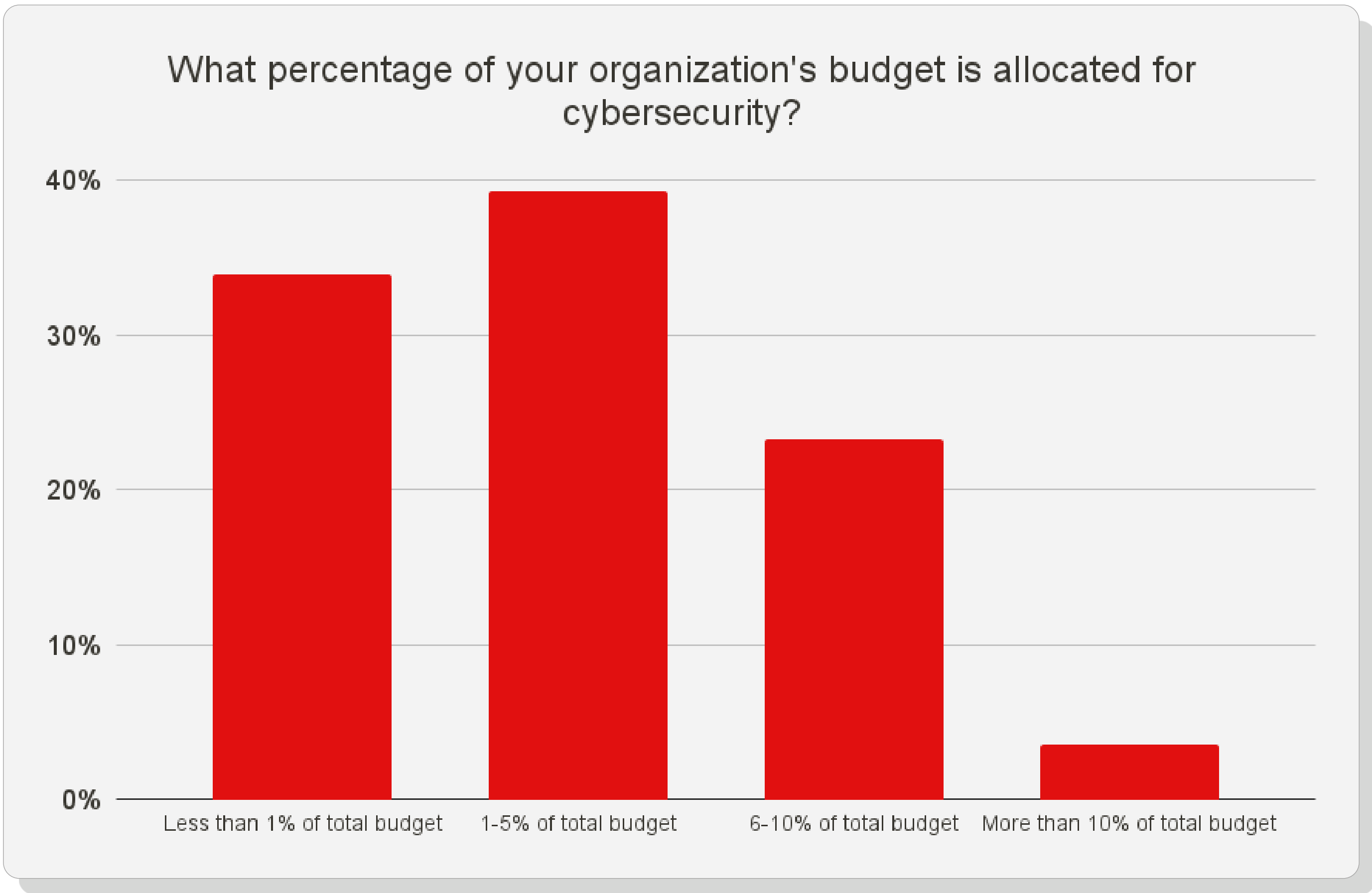
The survey highlights a diverse array of technologies employed, ranging from advanced threat detection to encryption, that underpin these cybersecurity strategies. Moreover, the survey illuminates the evolving landscape of communications with stakeholders in the event of a cyber incident, emphasizing the paramount importance of transparency and swift response. Additionally, the findings underscore the shifting landscape of Governance, Risk, and Compliance (GRC) responsibilities, reflecting an increasing integration of cyber risk management into overall business strategy.

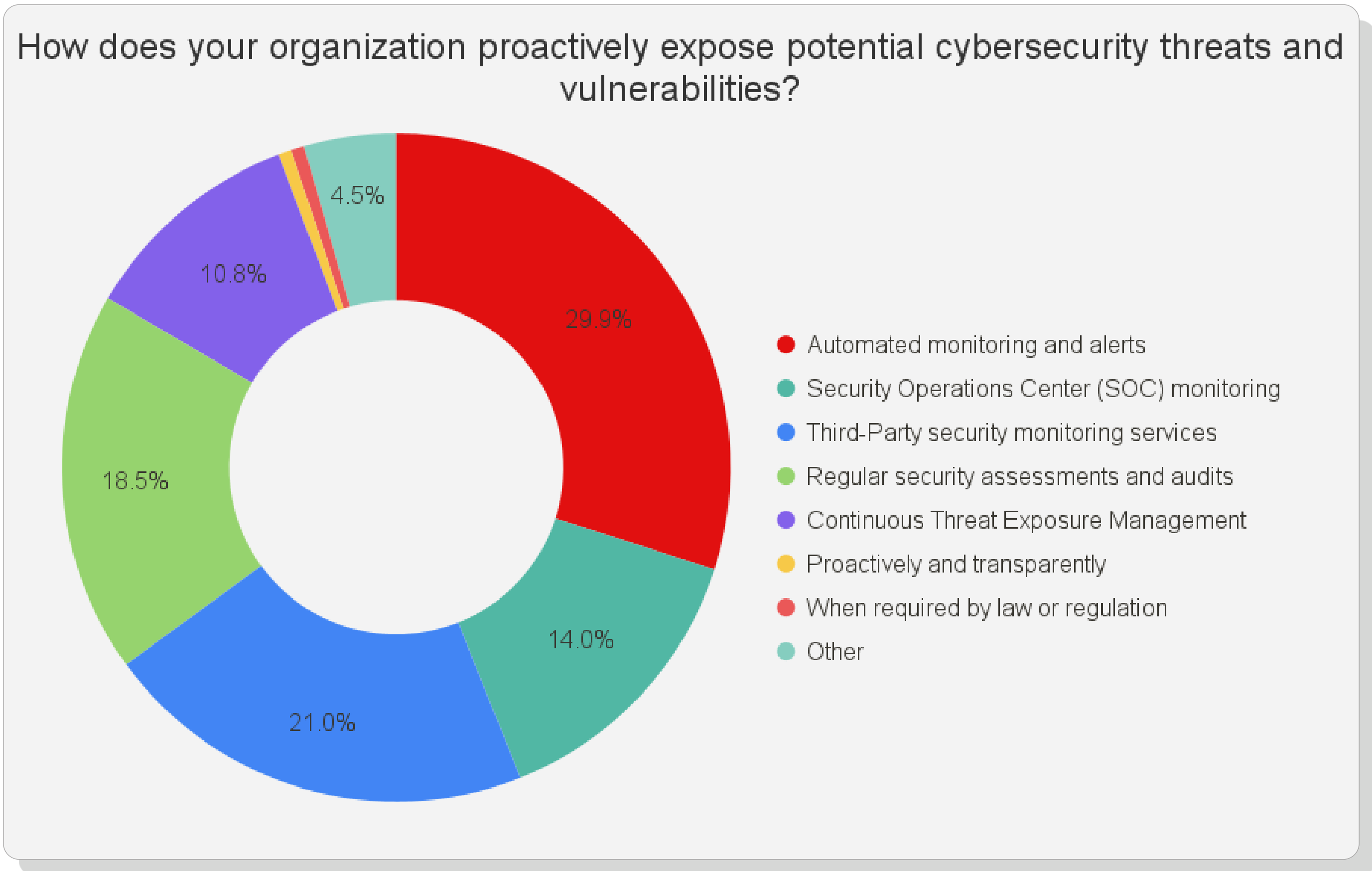

What best describes your seniority level within your organization?
25.5%
18.2%
56.4%
C Suite (CISO, CEO, CTO, etc.)
VP Level
Other, Intermediate

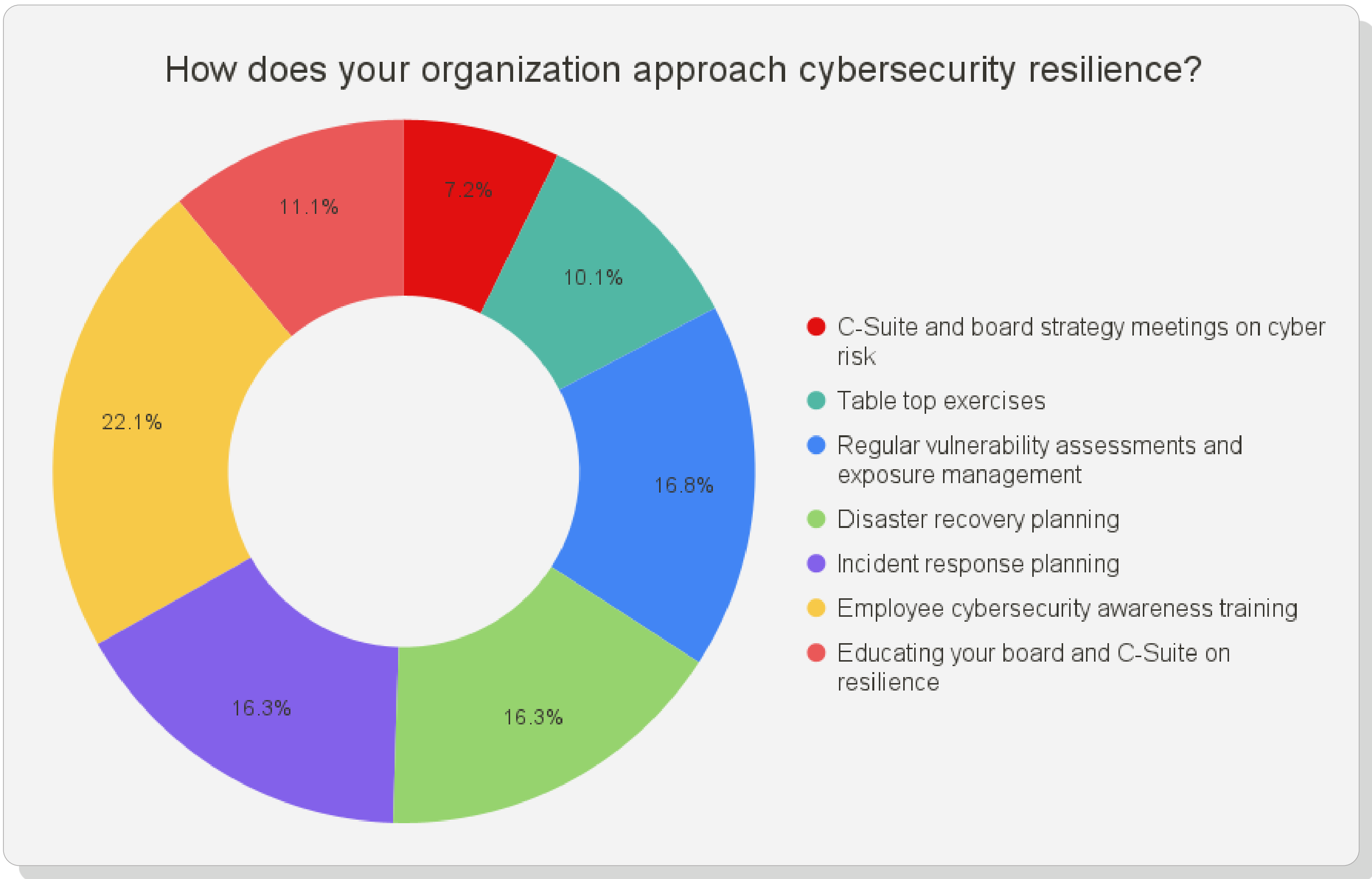

Does your organization have a written plan on how to communicate when a cybersecurity incident has occured?
60%
40%
20%
0%
Yes
No
Coming soon


Which cybersecurity framework does your organization currently employ?
NIST Cybersecurity Framework
ISO 27001/27002
COBIT
FISMA
CIS Controls framework
ENISA National Capabilities Assessment
FAIR Cyber Risk Framework
NIS2 Directive
Other
0%
10%
20%
30%

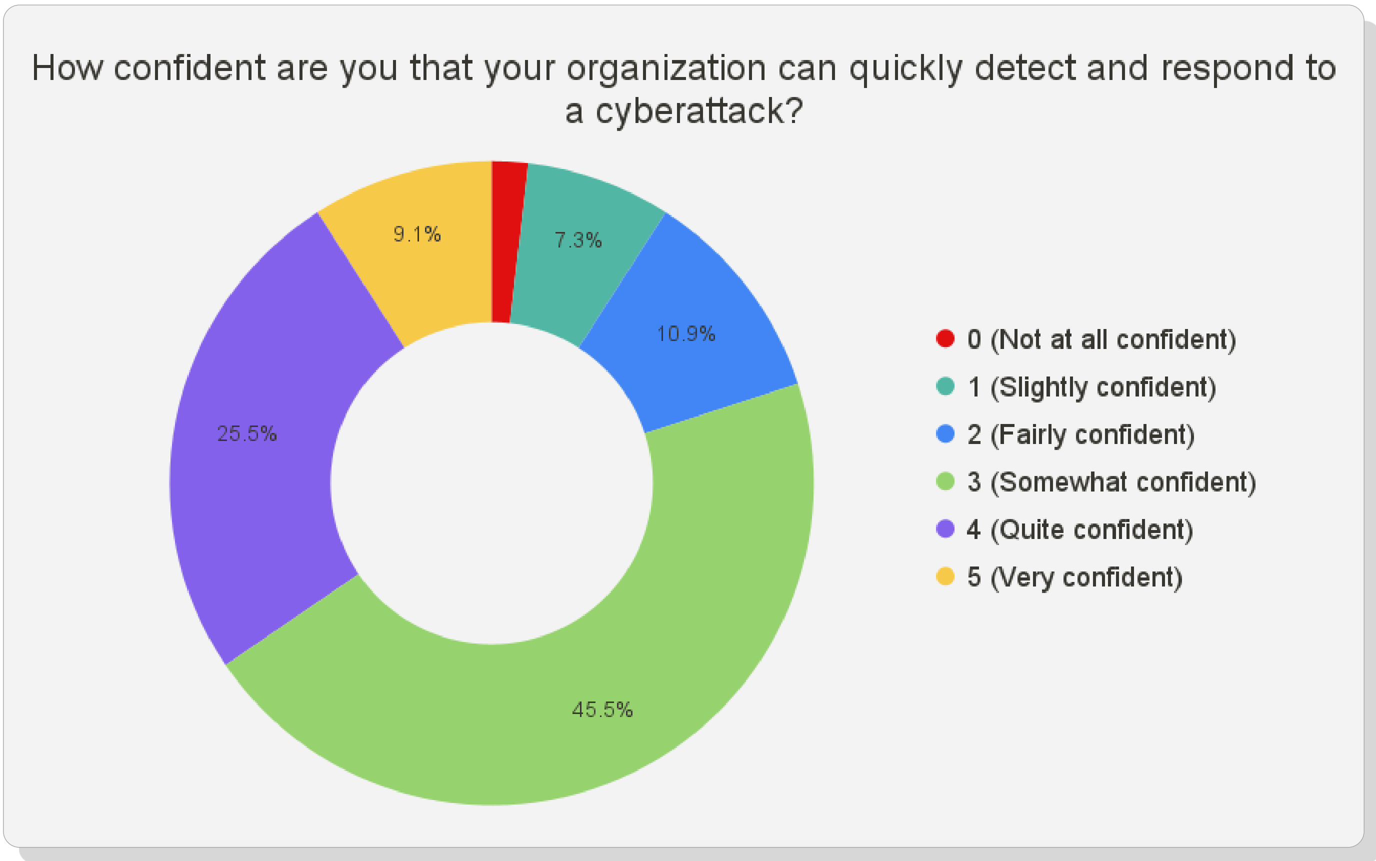

Does your organization have a dedicated cybersecurity team or department? If so, how many employees are on the team?
50%
40%
30%
20%
10%
0%
No
Yes, 1-10
Yes, 11-20
Yes, 21-50
Yes, 51-99
Yes, 100+
N/A


What percentage of your organization's budget is allocated for cybersecurity?
40%
30%
20%
10%
0%
Less than 1% of total budget
1-5% of total budget
6-10% of total budget
More than 10% of total budget

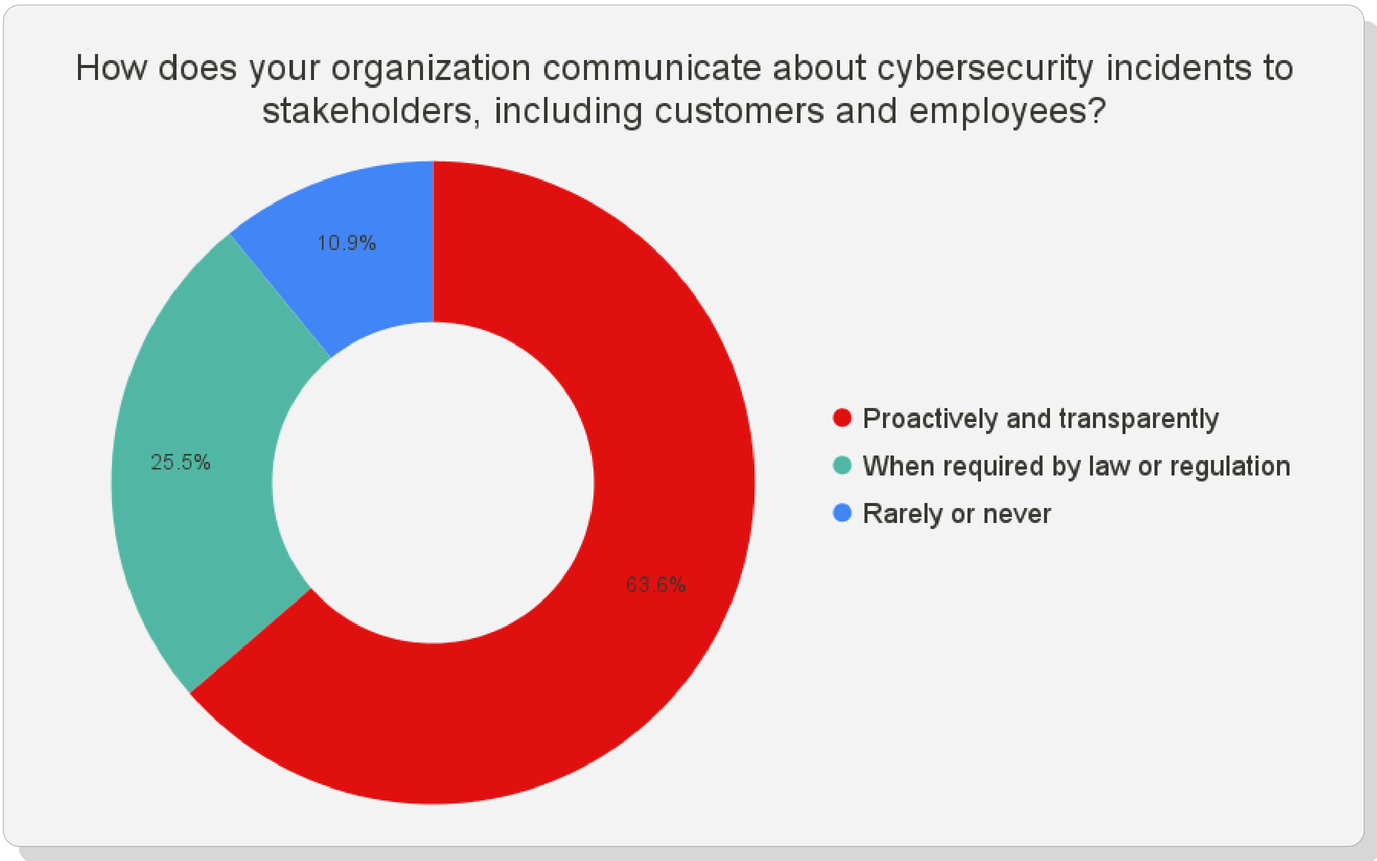

How does your organization proactively expose potential cybersecurity threats and vulnerabilities?
4.5%
10.8%
29.9%
18.5%
14.0%
21.0%
Automated monitoring and alerts
Security Operations Center (SOC) monitoring
Third-Party security monitoring services
Regular security assessments and audits
Continuous Threat Exposure Management
Proactively and transparently
When required by law or regulation
Other

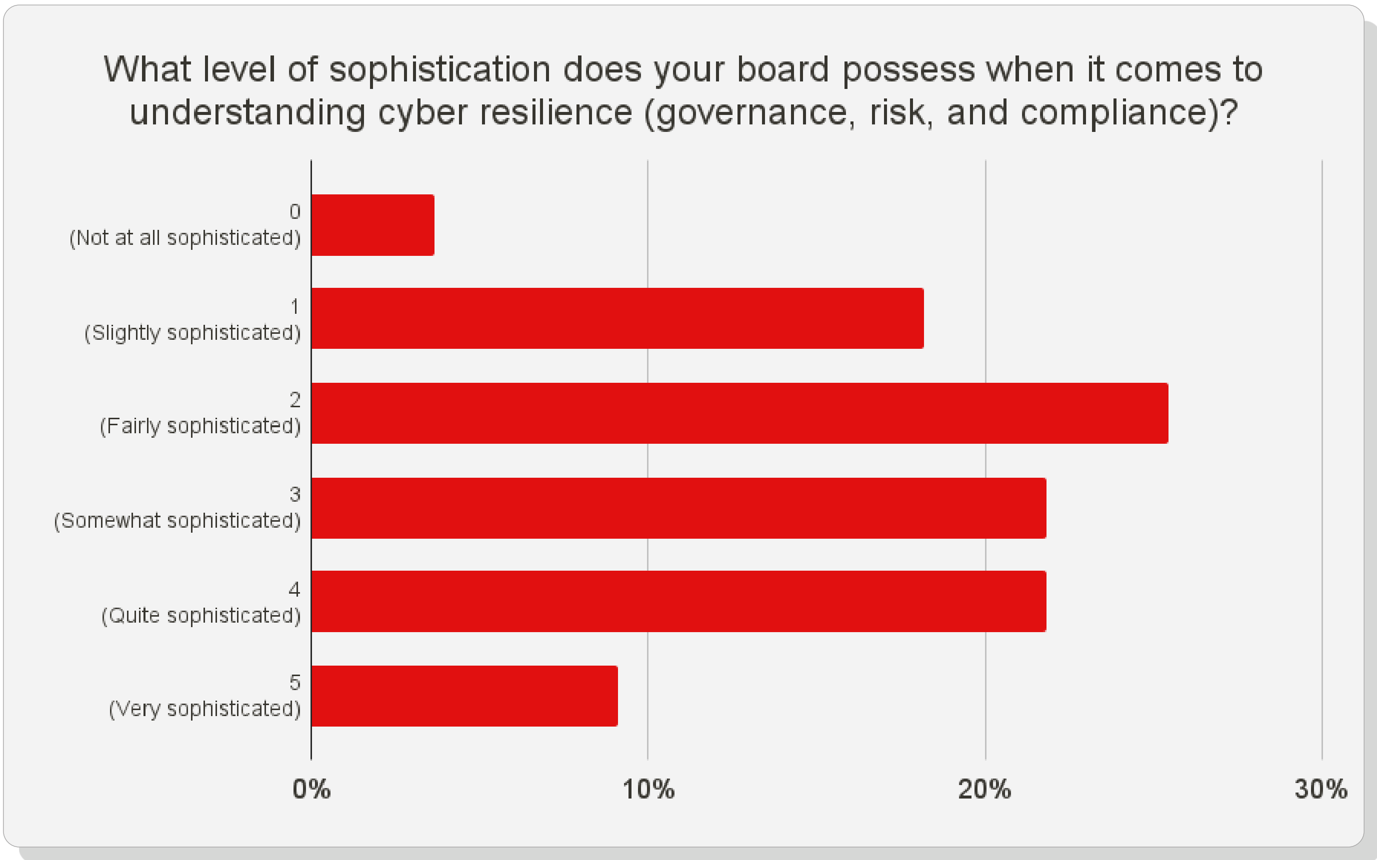

How does your organization approach cybersecurity resilience?
7.2%
10.1%
16.8%
16.3%
16.3%
22.1%
11.1%
C-Suite and board strategy meetings on cyber risk
Table top exercises
Regular vulnerability assessments and exposure management
Disaster recovery planning
Incident response planning
Employee cybersecurity awareness training
Educating your board and C-Suite on resilience


How often does your organization conduct a cybersecurity risk assessment?
Never
Monthly
Quarterly
Bi-annually
Annually
0%
20%
40%
60%


How confident are you that your organization can quickly detect and respond to a cyberattack?
9.1%
7.3%
10.9%
25.5%
45.5%
0 (Not at all confident)
1 (Slightly confident)
2 (Fairly confident)
3 (Somewhat confident)
4 (Quite confident)
5 (Very confident)

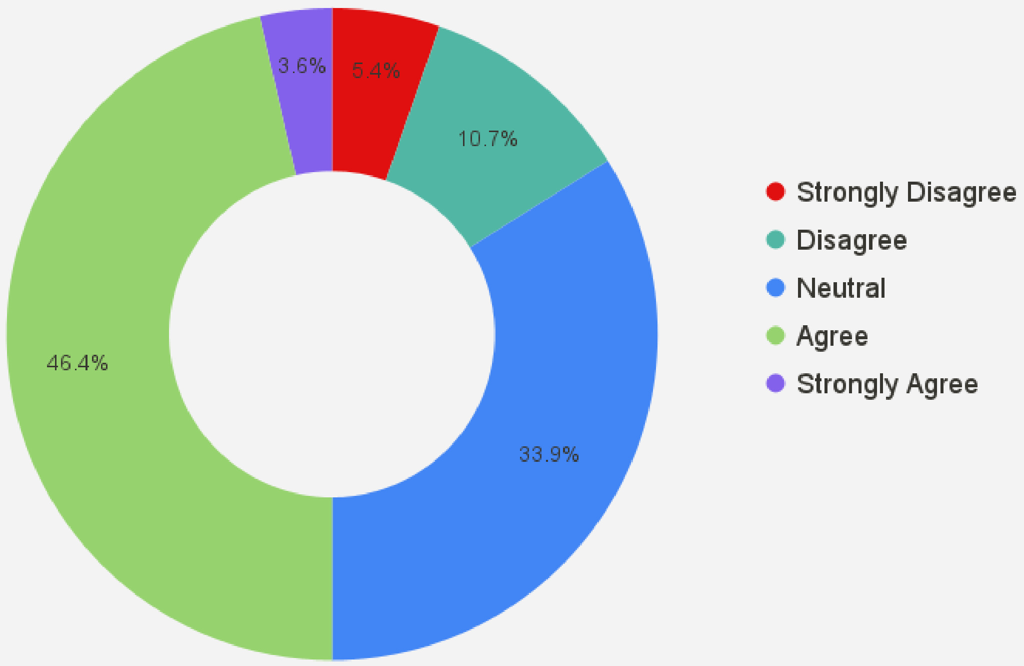

Has your organization faced significant challenges implementing cybersecurity resilience measures?
100%
75%
50%
25%
0%
Yes
No


How does your organization communicate about cybersecurity incidents to stakeholders, including customers and employees?
10.9%
25.5%
63.6%
Proactively and transparently
When required by law or regulation
Rarely or never

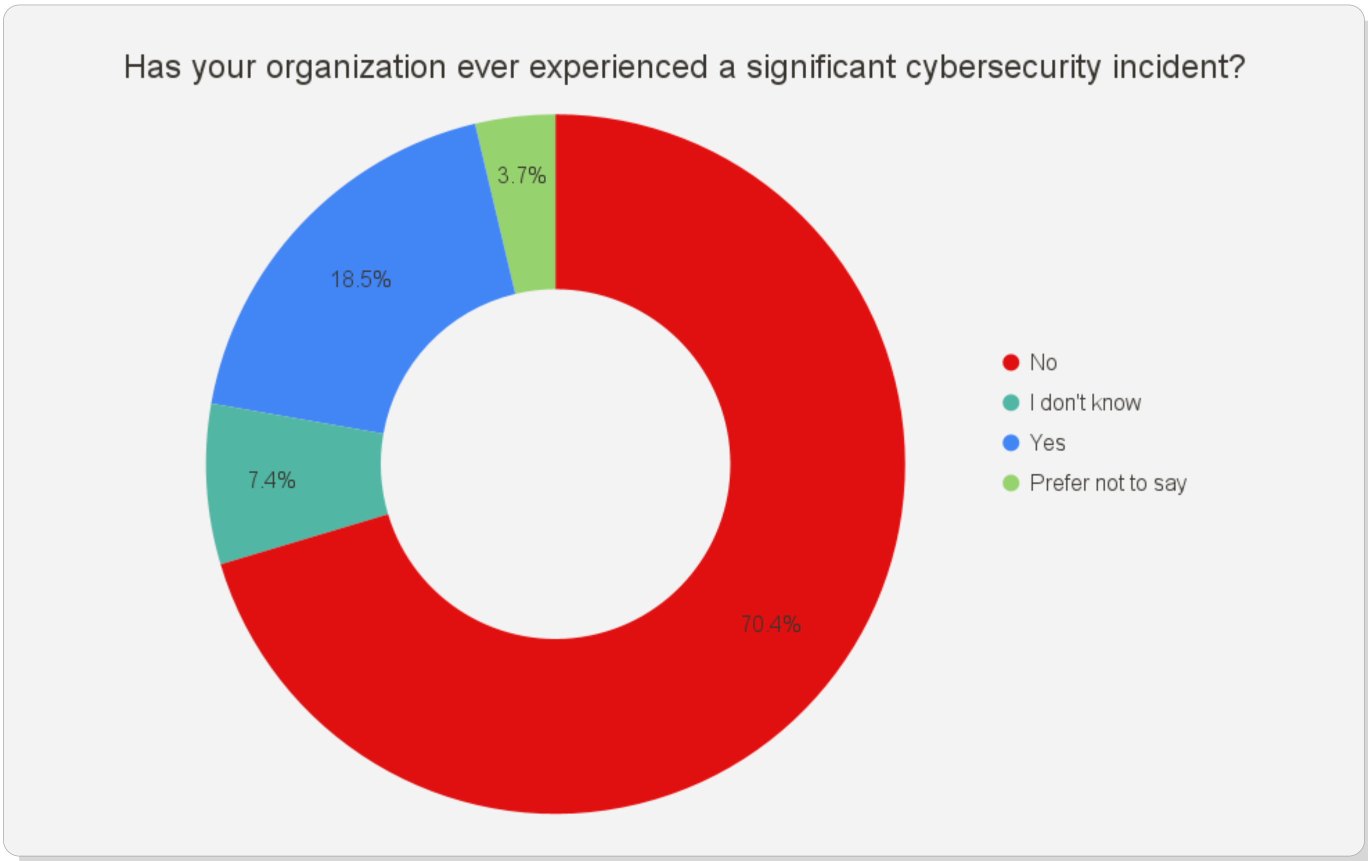

What level of sophistication does your board possess when it comes to understanding cyber resilience (governance, risk, and compliance)?
0 (Not at all sophisticated)
1 (Slightly sophisticated)
2 (Fairly sophisticated)
3 (Somewhat sophisticated)
4 (Quite sophisticated)
5 (Very sophisticated)
0%
10%
20%
30%

What is the biggest impediment you see to implementing cybersecurity resilience measures?

Broadly speaking, do you perceive cybersecurity vendors to be trustworthy partners?

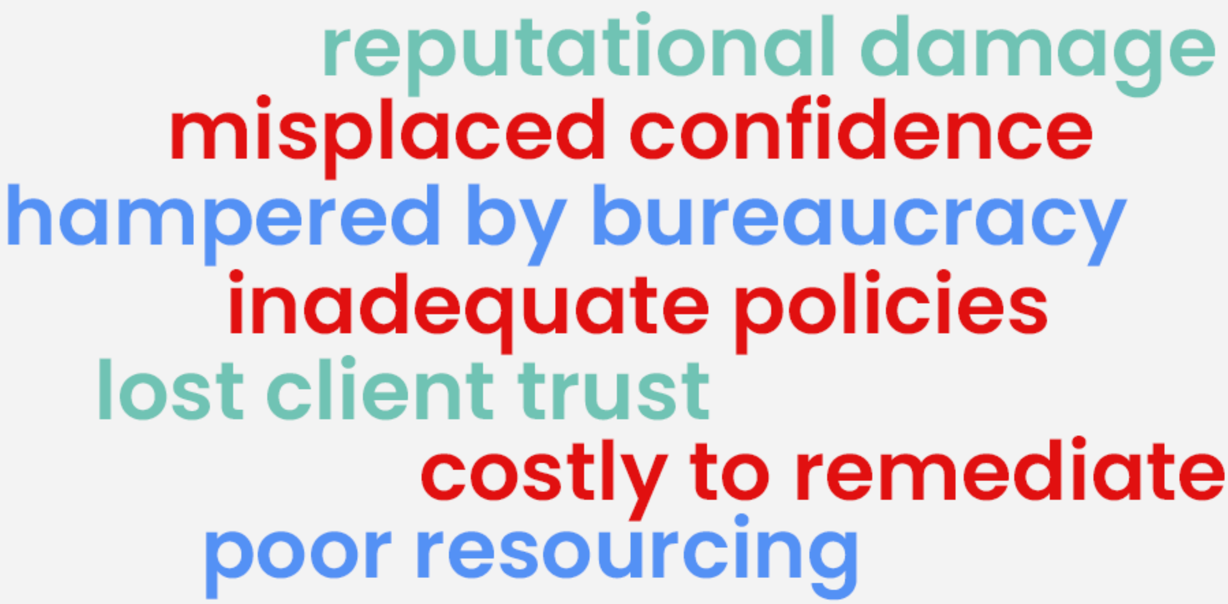


How confident are you that your organization's cybersecurity policies and procedures align with industry or regulatory standards and best practices?
40%
30%
20%
10%
0%
0
(Not at all confident)
1
(Slightly confident)
2
(Fairly confident)
3
(Somewhat confident)
4
(Quite confident)
5
(Very confident)



Has your organization ever experienced a significant cybersecurity incident?
3.7%
18.5%
7.4%
70.4%
No
I don't know
Yes
Prefer not to say

If you answered ‘yes’ to the previous question, what do you believe was the cause of why things went wrong?



Statement on methodology

The methodology of our survey on cyber resilience involved a rigorous and comprehensive approach aimed at gaining deep insights into the current state of cybersecurity practices. We designed a questionnaire that encompassed a wide range of topics related to cyber resilience, including risk management strategies, incident response protocols, technology investments, and governance frameworks.

The survey deployment process involved secure and confidential data collection methods, adhering to best practices for data privacy and protection. The responses were then analyzed using advanced data analytics techniques to derive meaningful and actionable insights, allowing us to paint an accurate picture of the cyber resilience landscape. The results of this survey serve as a valuable resource for organizations seeking to strengthen their cybersecurity strategies and adapt to the ever-changing threat landscape.

Conclusion

In 2023, the state of cyber resilience has reached a critical juncture, where organizations are navigating a digital landscape fraught with ever-evolving and cascading threats and challenges. As we navigate an increasingly interconnected digital landscape, the global state of cyber resilience in 2023 presents a mixed picture. Yet, as our research has uncovered, cyber resilience is no longer seen as a luxury but rather as an imperative for businesses and institutions of all sizes.

The year 2023 marks a time when proactive cybersecurity strategies, informed by data-driven insights, collaboration, and a commitment to emerging technologies, have started to become the bedrock of digital defense. Advances in technology and collaborative initiatives offer promise for better safeguarding systems and data, yet gaps in implementation, particularly in under-resourced regions or sectors, remain a significant concern. It is a year where organizations have recognized that cyber resilience demands continual adaptation and innovation.

The evolving global nature of cyber threats—ranging from sophisticated state-sponsored attacks to opportunistic cybercrime—demands continual vigilance and adaptability. As we look ahead, the commitment to strengthening cyber resilience remains paramount, ensuring that organizations can not only withstand the storms of the digital age but also thrive and innovate securely in a world where the only constant is change.

About the authors

Sean S Costigan PhD
Director of Cyber Policy
Red Sift

Dr. Sean Costigan is the Director of Cyber Policy at Red Sift Director overseeing and advising on the company's global cybersecurity policies and strategies. As an advisor to Red Sift's C-suite and senior leadership executives on cybersecurity matters, he provides continuous insights into the evolving threat landscape and in recommending appropriate action.

Sean is a respected cybersecurity industry professional who speaks frequently on cybersecurity and resilience around the world. An expert in emerging security challenges, he is a leader for NATO DEEP's cybersecurity capacity-building efforts, including Ukraine; co-author of the forthcoming PfPC/NATO Hybrid Threats and Warfare Curriculum; and Senior Advisor for the Emerging Security Challenges working group of the Partnership for Peace Consortium.

Sean is a graduate in the History of Science from Harvard University and earned his doctorate in cybersecurity from the University of Portsmouth, UK. Sean is a Professor at the George C. Marshall European Center for Security Studies, where he educates on the nexus of cybersecurity and hybrid threats. Sean is currently researching lessons learned from the cyber war in Ukraine and how to build a resilience strategy into organizations.

In 2023, Sean received the Serge Lazareff Prize for his contributions to the Office of Legal Affairs of NATO SHAPE.

About the authors

Rois Ni Thuama PhD

Director of Cyber Risk and Resilience, Red Sift

Rois Ni Thuama PhD is a doctor of law and subject matter expert in corporate & cyber governance, risk, and compliance. She is an award-winning cybersecurity expert and is the Head of Cyber Governance for Red Sift, one of Europe's fastest-growing cybersecurity companies.

Dr Ni Thuama works with key clients across a wide market spectrum providing expert insight to governments. Her most recent work was for the British Government for the Joint Committee on National Security Strategy (JCNSS) whilst her legal opinion has been sought by the US Government. Dr Ni Thuama delivered a presentation on legal implications at Fort McNair to US Department of Defence military experts which has shaped the understanding of AI in future conflicts. She is an Instructor for Cybersecurity, and on the Joint Command & Staff Course (OF-3) with the Irish Defence Forces. She works with boards and management across legal, financial, energy, and banking sectors to spread a contemporary understanding of cyber threats, risks, liabilities, and resilience across diverse audiences and stakeholders to drive effective change.

Acknowledgements

Red Sift would like to thank those who took the time to complete our State of Cyber Resilience LinkedIn survey and share their valuable and helpful insights.

We would also like to extend our gratitude to the following executives, experts, and staff members for sharing their time and considerable expertise:

- ***Mary Frantz****, Managing Partner, Enterprise Knowledge Partners*
- ***Harpreet Mann****, President, Amynta Trade Credit and Political Risk Solutions*
- ***Mihoko Matsubara****, Chief Cybersecurity Strategist, NTT*
- ***Owen Pierce,*** *Associate Director, Management Consulting Transformation Group, KPMG*
- ***Linda V. Priebe, JD, CIPP/E,*** *Partner, EU-US Data Privacy/Protection & Government Relations, Practus LLP*
- ***Helio Cabral SantAna,*** *CyberSecurity Operations Change Management, Forvia*
- ***Annie Searle,*** *Principle, Annie Searle and Associates*
- ***Gregory Touhill,*** *Director, Carnegie Mellon University Software Engineering Institute's CERT Division*
- ***Michal Wojnar,*** *Cyber Security Director, Cyber & Privacy at PwC CZ/CEE*

- ***Catrina Garner****, Regional Marketing Manager EMEA, Red Sift*
- ***Rachel Gray,*** *European Marketing Director, Red Sift*
- ***Ian Howells****, Chief Business Officer, Red Sift*
- ***John Klassen****, Sales Engineer, Red Sift*
- ***Nadim Lahoud****, VP of Strategy and Operations, Red Sift*
- ***Billy McDiarmid****, Product Director, Red Sift*
- ***Rebecca Warren****, Director of Product Marketing, Red Sift*

References

[i] IBM (2023). Cost of a Data Breach 2023. [online] IBM. Available at: https://www.ibm.com/reports/data-breach.

[ii] 2023 Mid-Year Cyber Security Report | Check Point Software. [online] Available at: https://pages.checkpoint.com/2023-mid-year-cyber-security-report.html

[iii] The Convergence of IT and Operational Technology: Cyber Risks to Critical Infrastructure on the Rise Cyber Signals. (2022). Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5daTD

[iv] Future of Industry Ecosystems: Shared Insights & Data | IDC Blog. [online] Available at: https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/.

[v] Irwin, L. (2023). List of Data Breaches and Cyber Attacks in 2023. [online] IT Governance UK Blog. Available at: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023.\

[vi] Simas, Z. (2023). Unpacking the MOVEit Breach: Statistics and Analysis. [online] Emsisoft | Cybersecurity Blog. Available at: https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/.

[vii] Cyber insurance risks and trends 2023 | Munich Re. [online] Available at: https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.html.

[viii] Cyber attacks set to become 'uninsurable', says Zurich chief. (2022). Financial Times. [online] 26 Dec. Available at: https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d.

[ix] NIST (2023). The NIST Cybersecurity Framework 2.0 (Draft). [online] csrc.nist.gov. Available at: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd.

[x] www.munichre.com. (n.d.). Cyber insurance risks and trends 2023 | Munich Re. [online] Available at: https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.html.

[xi] Boehm, J., Curcio, N., Merrath, P., Shenton, L. and Stähle, T. (2019). Risk Practice. [online] Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20risk%20based%20approach%20to%20cybersecurity/The-risk-based-approach-to-cybersecurity.pdf.

[xii] Boehm, J., Curcio, N., Merrath, P., Shenton, L. and Stähle, T. (2019). Risk Practice. [online] Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20risk%20based%20approach%20to%20cybersecurity/The-risk-based-approach-to-cybersecurity.pdf.

[xiii] Quinn, S., Ivy, N., Barrett, M., Feldman, L., Witte, G. and Gardner, R.K. (2021). Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. [online] doi:https://doi.org/10.6028/nist.ir.8286a.

[xiv] Crown Jewels Security Assessment.[online] Mandiant. Available at: https://www.mandiant.de/sites/default/files/2021-09/ds-crown-jewels-security-assessment-000369-2.pdf

[xv] www.lawsociety.ie. (n.d.). Plain English. [online] Available at: https://www.lawsociety.ie/gazette/in-depth/plain-english [Accessed 4 Oct. 2023].

[xvi] Verizon (2023). 2023 Data Breach Investigations Report. [online] Verizon Business. Available at: https://www.verizon.com/business/resources/reports/dbir/.

[xvii] Costigan, S. and Ni Thuama, R. (2023). 'Data Privacy, Cyber Compliance, and the (Surprising) Return on Investment' DATE Linda Priebe. [online] Available at: http://bit.ly/46IgFhS

[xviii] Allianz Commercial. (n.d.). Allianz Risk Barometer 2023 - Cyber incidents | AGCS. [online] Available at: https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2023-cyber-incidents.html.

[xix] Fallout The Reputational Impact of IT Risk. (n.d.). Available at: https://images.forbes.com/forbesinsights/StudyPDFs/IBM_Reputational_IT_Risk_REPORT.pdf.

[xx] ISACA. (2023). The State of Digital Trust. [online] Available at: http://www.isaca.org/digital-trust

[xxi] IBM (2023). Cost of a Data Breach 2023. [online] IBM. Available at: https://www.ibm.com/reports/data-breach.

[xxii] FedScoop. (2022). SolarWinds agrees to pay $26M to settle shareholder lawsuit over 2020 cyberattack. [online] Available at: https://fedscoop.com/solarwinds-agrees-to-pay-26m-to-settle-shareholder-lawsuit-over-2020-cyberattack/.

[xxiii] Federal Trade Commission (2022). Equifax Data Breach Settlement. [online] Federal Trade Commission. Available at: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

[xxiv] Data Protection Commission. (2022). Data Protection Commission. [online] Available at: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry.

[xxv] Capital One (2019). 2019 Capital One Cyber Incident | What Happened. [online] Capital One. Available at: https://www.capitalone.com/digital/facts2019/.

[xxvi] www.occ.gov. (2020). OCC Assesses $60 Million Civil Money Penalty Against Morgan Stanley. [online] Available at: https://www.occ.gov/news-issuances/news-

releases/2020/nr-occ-2020-134.html.

[xxvii] www.sec.gov. (2022). T-Mobile Form 8-K. [online] Available at: https://www.sec.gov/ix?doc=/Archives/edgar/data/0001283699/000119312522200065/d790999d8k.htm.

[xxviii] Koepke, P. (2017). Cybersecurity Information Sharing Incentives and Barriers. [online] Available at: https://cams.mit.edu/wp-content/uploads/2017-13.pdf.

[xxix] Predicts 2023: Cybersecurity Industry Focuses on the Human Deal. Gartner. (2023). Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025. [online] Available at: https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025#:~:text=Gartner%20predicts%20that%20by%202025

[xxx] Uptime Institute's 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening as Industry Efforts to Curb Outage Frequency Fall Short. [online] Available at: https://www.businesswire.com/news/home/20220608005265/en/Uptime-Institute%E2%80%99s-2022-Outage-Analysis-Finds-Downtime-Costs-and-Consequences-Worsening-as-Industry-Efforts-to-Curb-Outage-Frequency-Fall-Short#:~:text=According%20to%20Uptime%27s%202022%20Data.

[xxxi] Olson, A.B. (2022). 4 Common Reasons Strategies Fail. [online] Harvard Business Review. Available at: https://hbr.org/2022/06/4-common-reasons-strategies-fail.

[xxxii] Vi and Oltsik, J. (2023). The Life and Times of Cybersecurity Professionals Volume VI 1 The Life and Times of Cybersecurity Professionals The Life and Times of Cybersecurity Professionals Volume VI 2. [online] Available at: https://www.techtarget.com/esg-global/wp-content/uploads/2023/09/The-Life-and-Times-of-Cybersecurity-Professionals-Volume-VI.pdf

[xxxiii] Townsend, K. (2022). Vulnerability Management Fatigue Fueled by Non-Exploitable Bugs. [online] SecurityWeek. Available at: https://www.securityweek.com/vulnerability-management-fatigue-fueled-non-exploitable-bugs/

[xxxiv] World Economic Forum. (2023). Global Security Outlook. [online] Available at: https://www.weforum.org/reports/global-cybersecurity-outlook-2023/.

[xxxv] Coutinho, S., Bollen, A., Weil, C., Sheerin, C., Silvera, D., Donaldson, S. and Rosborough, J. (2023). Cyber security skills in the UK labour market 2023 Findings report. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1173325/Cyber_security_skills_in_the_UK_labour_market_2023.pdf.

[xxxvi] Costigan, S. (2023). Guardians of the Cyberverse: Building a Resilient Security Culture. Dark Reading. [online] 22 Sep. Available at: https://www.darkreading.com/vulnerabilities-threats/guardians-of-the-cyberverse-building-a-resilient-security-culture [Accessed 22 Sep. 2023].

[xxxvii] Storsbergen, M. (2023). Cyber Shame: The Cyber Word of the Year. [online] Guardey. Available at: https://www.guardey.com/cyber-shame-the-cyber-word-of-the-year/

[xxxviii] Stupp, C. (2023). Biotech CEO Gets Hands-On After Cyberattack to Protect Business. Wall Street Journal. [online] 3 Jul. Available at: https://www.wsj.com/articles/biotech-ceo-gets-hands-on-after-cyberattack-to-protect-business-9c6d08fe

[xxxix] AR-IN-A-BOX. (2023). [online] ENISA. Available at: https://www.enisa.europa.eu/topics/cybersecurity-education/2023-ar-in-a-box-material/cyber-awareness-program_03-online.pdf.

[xl] Smart cyber How AI can help manage cyber risk Cyber. (2022). Available at: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-smart-cyber.pdf.

[xli] Microsoft. (2019). Detecting Cyber Attacks Using Anomaly Detection With Explanations And Expert Feedback . [online] Available at: https://www.microsoft.com/enus/research/uploads/prod/2019/06/ADwithGraderFeedback.pdf

[xlii] Kovacs, E. (2023). Dangling DNS Used to Hijack Subdomains of Major Organizations. [online] SecurityWeek. Available at: https://www.securityweek.com/dangling-dns-used-to-hijack-subdomains-of-major-organizations/ [Accessed 4 Oct. 2023].

[xliii] Schweitzer, F. (2023). Thousands of Organizations Vulnerable to Subdomain Hijacking – Certitude Blog. [online] certitude.consulting. Available at: https://certitude.consulting/blog/en/subdomain-hijacking/.

[xliv] Petkauskas, V. (2023). Starlink outage over certificate 'inexcusable' . [online] Cybernews. Available at: https://cybernews.com/news/starlink-outage-certificate-elon-musk/.

[xlv] Threat Horizons Report 2023. (2023). [online] Google. Available at: https://services.google.com/fh/files/blogs/gcat_threathorizons_full_jul2023.pdf

[xlvi] FBI. (2012). Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies. [online] Available at: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[xlvii] www.sec.gov. (2023). SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. [online] Available at: https://www.sec.gov/news/press-release/2023-139.

[xlviii] SEC. (2023). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. [online] Available at: https://www.sec.gov/files/rules/final/2023/33-11216.pdf.

[xlix] www.sec.gov. (2021). SEC.gov | SEC Charges Pearson plc for Misleading Investors About Cyber Breach. [online] Available at: https://www.sec.gov/news/press-release/2021-154.

[l] Melchiondo, K.R. (2023). SEC's New Cyber Incident Disclosure Requirements Will Go Into Effect in December | Privacy Portal Blog | Insights & Events | Bilzin Sumberg. [online] www.bilzin.com. Available at: https://www.bilzin.com/we-think-big/insights/publications/2023/07/secs-cyber-incident-disclosure-requirements

[li] Rose, R., Dziekanowski , T. and Watkin-Child , A. (2023). SEC Cybersecurity Rule Leans on Materiality and Reasonableness. [online] news.bloomberglaw.com. Available at: https://news.bloomberglaw.com/us-law-week/sec-cybersecurity-rule-leans-on-materiality-and-reasonableness

[lii] Ni Thuama, R. and Costigan, S.S. (2023). DORA - Understanding the New Regulatory Framework on Digital Operational Resilience. Social Science Research Network. doi:https://doi.org/10.2139/ssrn.4549564.

[liii] NIST (2023). The NIST Cybersecurity Framework 2.0 (Draft). [online] csrc.nist.gov. Available at: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd.

[liv] European Union (2022). Cyber Resilience Act | Shaping Europe's digital future. [online] digital-strategy.ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[lv] The World Bank (n.d.). Cybersecurity. [online] World Bank. Available at: https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview.

[lvi] www.cisa.gov. (2023). Shifting the Balance of Cybersecurity Risk: Security-by-Design and Default Principles | CISA. [online] Available at: https://www.cisa.gov/news-events/alerts/2023/04/13/shifting-balance-cybersecurity-risk-security-design-and-default-principles.

[lvii] Payment Card Industry Data Security Standard Requirements and Testing Procedures Version 4.0. (2022). Available at: https://www.commerce.uwo.ca/pdf/PCI-DSS-v4_0.pdf.

[lviii] Dmarc.org. (2015). dmarc.org – Domain Message Authentication Reporting & Conformance. [online] Available at: https://dmarc.org/.

About Red Sift

Red Sift enables organizations to anticipate, respond to, and recover from cyber attacks while continuing to operate effectively. The award-winning Red Sift application suite is the only integrated solution that combines four interoperable applications, internet-scale cybersecurity intelligence, and innovative generative AI that puts organizations on a robust path to cyber resilience.

Red Sift is a global organization with offices in North America, Australia, Spain, and the UK. It boasts a global client base across all industries, including Domino's, ZoomInfo, Athletic Greens, Pipedrive, and top global law firms. Red Sift is also a trusted partner of Entrust, Microsoft, Cisco and Validity, among others. **Learn more at redsift.com.**

RED SIFT

redsift.com