Navigating 2024's Cyber Landscape

A Guide to Confident Cybersecurity

iventure

Contents

Introduction

This evolving technological landscape necessitates robust cybersecurity measures to mitigate potential security risks. The heart of understanding these technological shifts lies in balancing operational efficiency with stringent security practices.

With every advancement in automation and software development, the necessity for strong security and adaptation to emerging vulnerabilities becomes increasingly vital.

Cybersecurity threats have steadily increased over the years, with data breaches averaging a cost of

$4.35M

to businesses in 2022. In 2024, we expect to see even more sophisticated and subtle threats.

Consequently, a proactive and anticipatory approach to cybersecurity is more crucial than ever.

After years of fighting for their place among the executive team, today's security leaders are seeing increased collaboration among departments and increased budgets to work with, given the nature of what's at stake. This culture shift is not only required but welcomed. In places where IT integrates at every level of a business, cybersecurity is top of mind, and resilience and awareness become the order of the day.

Oftentimes this seems like a daunting prospect and one that can appear cost-prohibitive, yet that's not necessarily the case. The good news? Every organization can take small, proactive measures to protect themselves against risk and future-proof their organizations.

In this whitepaper, we'll break down what organizations can do now and in the future to stay one step ahead of the trends and associated threats. We'll help you unravel some of the intricacies of the cybersecurity landscape in 2024, identifying the challenges and opportunities that will arise as a result of increased advancements in technology.

The Evolving Technology Landscape

The technology landscape is in perpetual motion, responding to and driving new trends, new threats, and new opportunities. As a result, a variety of factors will shape the cybersecurity landscape. To the surprise of no one, there is an increase in cloud and remote infrastructure dependence, driven by the COVID-19 pandemic and the resulting hybrid workforce. The burgeoning role of AI in the technology sector is one we're all paying attention to, which combined with the factors above, will see an increase in more sophisticated and persistent attacks. Although this sounds a little ominous, we're here to help you break down the key factors that stand to be pivotal.

Increasing Cloud and Remote Infrastructure Dependence

The last few years have seen a meteoric rise in organizations depending on both cloud infrastructures and remote work models. The combination of technological innovation has redefined organizational landscapes and catalyzed an entirely new way of working and managing IT infrastructure.

Hybrid cloud infrastructures allow organizations to be more flexible and adaptable, and to scale far more efficiently, but they also expand the attack surface, offering increased vulnerabilities for threat actors to exploit. As a result, these working practices will be pivotal when it comes to thinking about cybersecurity in 2024.

Remote and Hybrid Work Infrastructures

The COVID-19 pandemic acted as the catalyst for a pre-existing trend that turbocharged the popularity and availability of remote work models. Although some businesses have returned completely to in-person work, the majority of organizations are now set up for hybrid work in a way that has reshaped the security landscape. Examples of this include remote working seeing an increase in cyber-attacks involving ransomware and magnified vulnerabilities in VPN's. This represents a dramatic shift, and while many businesses were slow to adapt their security requirements, 2024 will see an urgency to respond to the wider attack surface that remote and hybrid work presents.

The dynamic and flexible nature of the workforce this year will demand more robust security measures and a different mindset to safeguard dispersed endpoints and foster a seamless balance between accessibility and security.

> **"Once you move home, we have some lack of control. Coupled with moving to the cloud — there are a lot of shifts there. The disparity between where people can work and what is on those networks at home…that's a big change that's impacted things from a cybersecurity standpoint"**
>
> — Aaron Ward, iVenture, CISO

The Role of AI and Emerging Technologies

Given its importance in the wider world of IT, it is no surprise that AI stands to be one of the most influential and important aspects of innovation, affecting technology and subsequently, cybersecurity.

The potential to use AI from a cybersecurity standpoint is enormous, adding an unprecedented ability to predict and mitigate threats and provide resilience to an organization's defenses. And while artificial intelligence (AI) offers incredible applications for cybersecurity, it can bring with it new attack vectors that are not always fully understood. Suffice it to say that AI is here to stay, and we anticipate its evolution as something to watch and maneuver in the years to come.

The Rise of Sophisticated Cyber Threats and Attacks

As noted above, the year will see a proliferation of cyber threats, from Advanced Persistent Threats and ransomware to supply chain attacks.

Generative AI will be used in phishing attempts via email and SMS, as well as other social engineering methods including voice and video, making these attacks seem more authentic and harder to guard against.

Businesses will need to maintain a state of constant vigilance and be increasingly adaptable and agile to stay safe.

The Times are (Rapidly) Changing: Cybersecurity Threats

These transformative shifts don't just have an impact on organizations' security postures.

The increased ability and sophistication of threat actors to identify and exploit weaknesses in an organization's perimeter defenses prompts the need for more adaptive security measures, as well as increasingly robust incident response frameworks.

But more importantly, it will require a cultural shift and a change of mindset, instilling cybersecurity consciousness across all levels of an organization. Cybersecurity can no longer be seen as 'just an IT issue', but must be reimagined as a fundamental part of business strategy — something proactive and anticipatory, and embedded in operational processes.

Zero Trust and Connected Ecosystems

2024 will see an increased emphasis on Zero Trust and a redefinition of traditional, perimeter-based security measures.

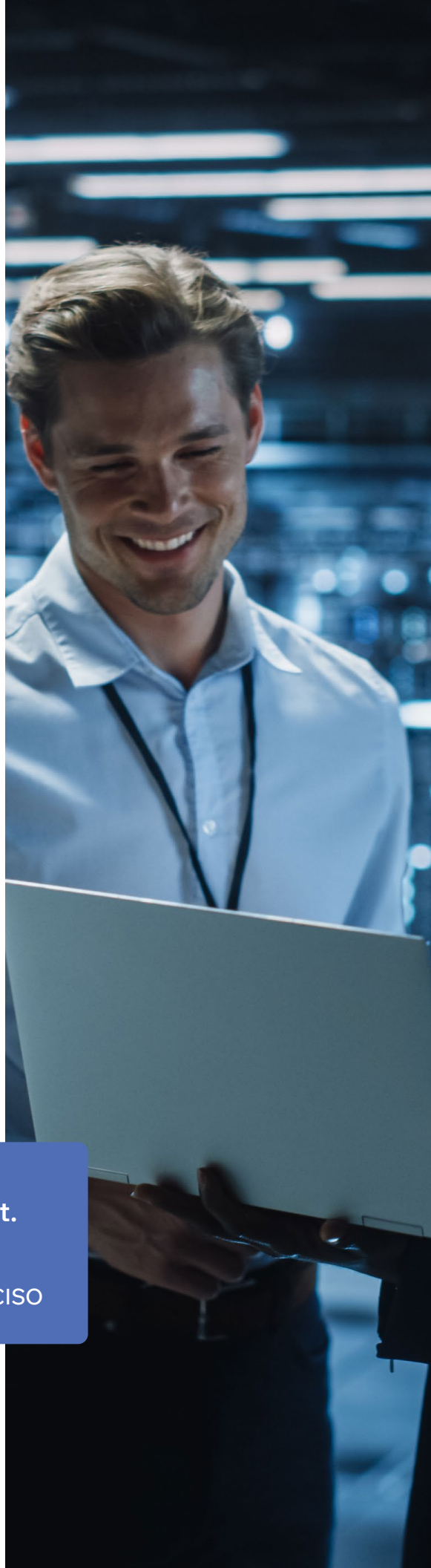
As digital (and even physical) ecosystems become far more connected and boundaries begin to blur, threats can come from anywhere and implicit trust in internal users will no longer be feasible. Zero Trust emphasizes continuous verification, irrespective of user or location. As local infrastructure gives way to a far larger and more dispersed ecosystem of apps, software, and users, putting trust in vendors will be a far more risky proposition.

The Maturation and Challenges of Generative AI in Cybersecurity

Generative AI exploded into the public consciousness in 2021 with the release of a slate of AI language and image models.

The last few years have seen a maturation in the abilities of AI, driving innovation across the IT sector and bringing remarkable capabilities and new challenges to the world of cybersecurity. As a result, AI will be one of the defining trends of 2024.

> **"Chat GPT can be your friend, but it's also a beast. It can be used against you as well."**
>
> — Aaron Ward, iVenture, CISO



Generative AI empowers security measures with an unprecedented level of predictive analysis and threat detection. But it also introduces a wide variety of complexities, from an expanded threat surface to a slate of ethical considerations. Many organizations are quick to integrate the use of AI into their operations, without understanding where information is going and who has access to it.

> **"I don't want to put sensitive data into AI, I don't want to put anything that could be used against me or any identifying information."**
>
> — Aaron Ward, iVenture, CISO

The Continuous Evolution of Malicious Actors and Defense Strategies

We are likely to see an even more pronounced evolution of the ways that bad actors frame their attacks, as technologies like AI make it harder than ever to identify threats given it can be more challenging to determine the legitimacy of apps, software, and IT players.

As technology develops, cyber adversaries are often at the cutting edge of innovation as they discover and develop ever more sophisticated tactics for breaching defenses and sniffing out vulnerabilities.

These threats underscore a pivotal shift in the way cybersecurity will work going forward. Embracing and addressing these issues isn't just a good idea, it's a strategic imperative.

Adapting Strategies to Mitigate Potential Risks

So what can businesses do on a practical level to mitigate the risks of cyber attacks? As cyber threats become more sophisticated and more frequent, the key to successful defense strategies is proactivity. Constant monitoring and end-user training to make an organization more resilient lays the foundations, while taking action to predict and prevent attacks before they take place is the most effective way to fortify its cybersecurity posture. Mitigating cyber risks is essential, so let's dive into strategies.

Proactive Defense

The key to cybersecurity in 2024 will be moving from reactive to preemptive security measures.

Trends like Zero Trust mark a fundamental transformation in cybersecurity paradigms and show that businesses are embracing elements like predictive analysis, threat intelligence, and real-time monitoring to shore up their defenses. Thwarting potential threats before they materialize cuts out a lot of the risk involved in cyber attacks and helps businesses protect themselves more effectively.

> **"In the past, we were getting cries for help, reactive ones. And they weren't even customers at the time. They were just calling around to see who could help. But fortunately, we're not getting any of those right now. Now we are getting more of the proactive ones."**
>
> — Aaron Ward, iVenture, CISO

End-User Training and Security Awareness

Raising awareness of cybersecurity issues amongst your staff and training them to be more resilient and protect themselves and the company against threats is the most cost-effective and just effective-effective cybersecurity measure around.

Human error is one of the most significant gateways for cyber threats, but it also represents an area that is easy to fortify and can be vital in the fight against malicious actors. Leveling up staff and cultivating a culture of cybersecurity awareness is a huge part of any security arsenal and a great way to take a proactive approach to security.

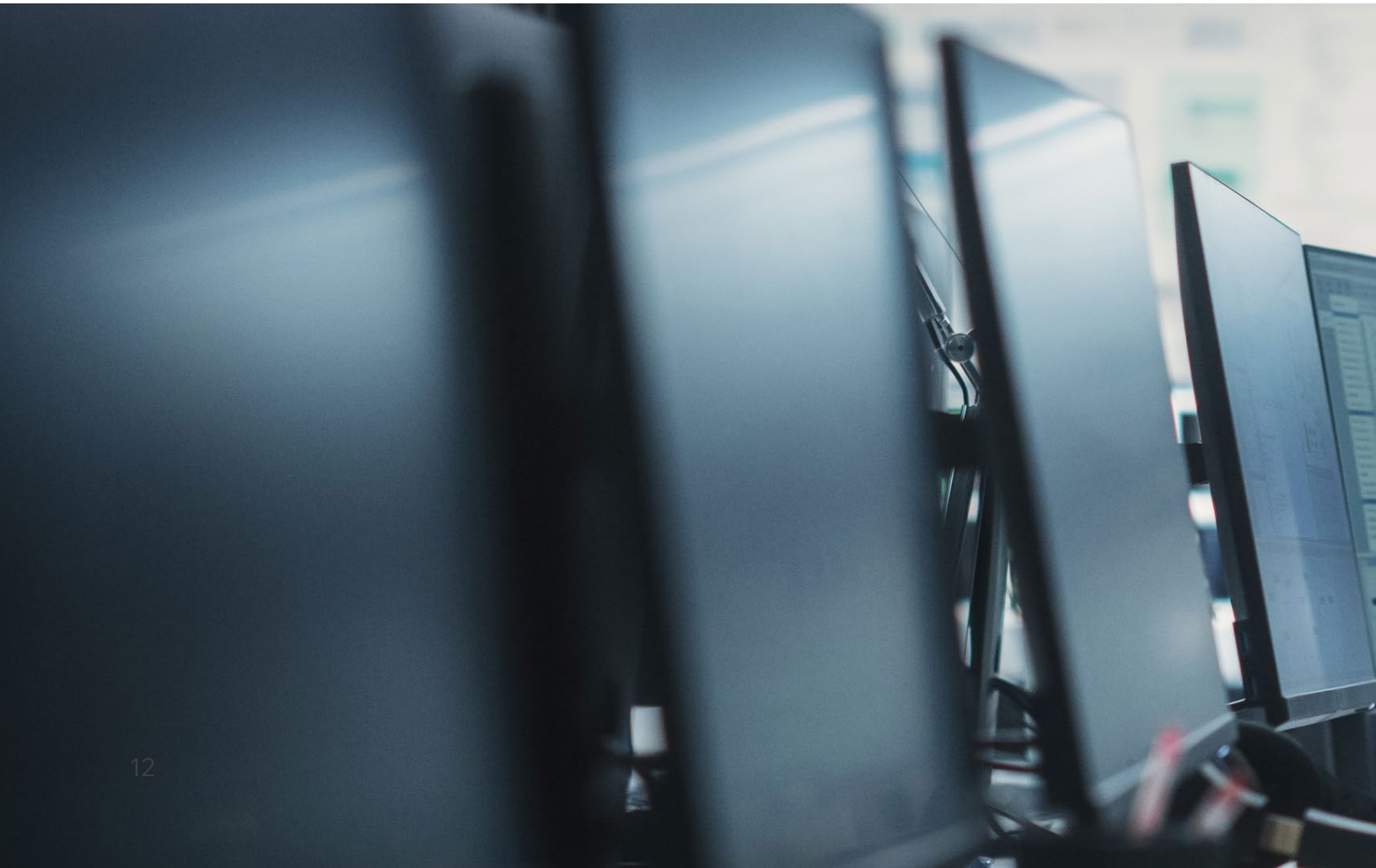
> **"The biggest bang for your buck when it comes to security defenses is end-user training."**
>
> — Aaron Ward, iVenture, CISO

Here are some ways to drive this culture change:

1. Improve employee awareness about the importance of securing information, of legitimizing third-party requests, two-factor authentication, and protecting private and personal information.

2. Promote cross-functional collaboration across all departments when it comes to security. When engineering, IT, and marketing work together, it can prevent smaller security incidents from spiraling out of control, help to quickly remediate the issues that do arise, and generally create a more adaptable environment, essential to surviving the IT and cybersecurity landscape.

3. Reach out to a certifiable third-party partner who has deep expertise in crafting security strategies, providing training, and acting as a resource for organizations.



Continuous Risk Management and Assessment

Cyber threats are always changing, so cybersecurity efforts need to shift and change to match them. This means that businesses always have to monitor current and potential threats, assess and manage risk, and develop robust incident response plans.

This ensures an agile, responsive, and effective security infrastructure that can adapt quickly to threats as they evolve and grow. Updates and tests aren't just a nice-to-have (or an annoying pop-up getting in the way of day-to-day work). They are an essential part of protecting a business in a time of constantly changing threats. Security protocols go from effective to obsolete faster than ever before, so regular updates and rigorous testing are imperative if you want to patch vulnerabilities and stay safe in the face of emerging threats.

> "There's never a destination. It's a journey. You're never going to have enough to be able to say, 'I am totally protected'. You need to kind of keep looking at what else is the business doing and where else can protection be done."
>
> — Aaron Ward, iVenture, CISO

Here are some ways that organizations can proactively manage their cybersecurity exposures:

Have offline, regularly tested, and segregated backups. In the event of a security breach, it's not just leaked information that can pose a challenge, but a paralyzed technology platform, preventing work from being done. Ensuring segregation in data storage and operability helps to ensure business continuation in the event of an attack.

Ensure maintenance responsibility is clear within the organization and conduct regular vulnerability tests.

Run pressure tests on the systems and instigate exercises across all levels of the organization, to ensure readiness.

Leveraging AI Technology

The potential of AI and automation in the cybersecurity sphere has only just begun to be explored, and 2024 will see exponential growth in its application. These innovative technologies stand to become linchpins in augmenting cybersecurity efforts, thanks to AI-driven data analysis and automated threat detection, response, and mitigation.

Though time will tell exactly how AI will transform the technology industry and by proxy, cybersecurity, it's clear that it will help organizations move more quickly in the case of incidents, from detection to protection to mitigation to business continuity.

Engaging Trusted Security Partners for Comprehensive Solutions

Teaming up with trusted cybersecurity experts is one of the best strategies to deal with the intricate and complex cybersecurity landscape in front of us.

From the latest technology to bespoke, comprehensive strategies tailored to specific organizational needs, a trusted partner is a key part of making a business more resilient.

> **"Cyber defenders will use gen AI and related technologies to strengthen detection, response, and attribution of adversaries at scale, as well as speed up analysis and other time-consuming tasks such as reverse engineering."**
>
> — Cybersecurity Forecast 2024, Google Cloud

Conclusion

2024 looks set to be a year of huge changes in the IT landscape in general. With businesses increasingly dependent on cloud infrastructure and beginning their explorations of the possibilities of AI, there is an extraordinary amount to be excited about.

With change, however, comes new challenges, and the persistent evolution of cyber threats, alongside the complexity of new working models and new work infrastructures will require transformation and adaptability when it comes to cybersecurity.

At iVenture Solutions, we stand ready to act as a trusted partner, helping businesses navigate the complex landscape and become stronger and more resilient across the board. Our expertise and innovative solutions are tailored to make the world of InfoSec easier and more understandable and to empower organizations to embrace proactive strategies and fortify their defenses.

Contact us today for a personal assessment to explore how customized IT solutions can elevate your business.

iventure

iVentureSolutions.com