DigitalXRAID
CYBER SECURITY EXPERTS

SECURING OUR DIGITAL FUTURE

# Navigating the Challenges and Opportunities of Cybersecurity

**Today's challenges require us to be innovative, resilient, and proactive**

The rapid development of digital technology has brought significant benefits to society, but it also poses serious challenges to the national and economic security interests of free and open societies.

In the next decade, the cybersecurity landscape will be shaped by a range of technological advancements and challenges that require us to be innovative, resilient, and proactive.

# The Cyber Space in Ten Years' Time

The cyber space is constantly evolving, and it is difficult to predict its future development.

However, we can expect that the number of internet users and connected devices will continue to increase.

This will bring new opportunities for businesses and individuals, but also create new vulnerabilities and threats.

As we move towards a more connected world, cybersecurity will become even more critical, and we need to develop innovative solutions to ensure that the cyber space remains free, open, and democratic.

The digital age has brought unprecedented connectivity and opportunities for businesses and individuals across the world.

However, as the number of internet users and connected devices increases, so does the risk of cyberattacks.

In the next decade, the cybersecurity landscape will be shaped by a range of technological advancements and challenges that require us to be innovative, resilient, and proactive.

According to a recent report, global cybercrime costs are expected to reach $10.5 trillion annually by 2025.

This highlights the increasing importance of cybersecurity in the digital age. As technology continues to advance, so do the capabilities of cyber criminals, making it even more important for individuals and businesses to take proactive measures to protect themselves.

One of the most effective measures that businesses can take to protect themselves from cyberattacks is to outsource their cybersecurity needs.

Outsourcing cybersecurity to a trusted provider has become an increasingly popular solution for businesses of all sizes in recent years.

**Cybercrime costs are expected to reach $10.5 trillion annually by 2025**

# Here are some of the benefits that businesses can expect from outsourcing their cybersecurity needs:

## Expertise and experience

Cybersecurity providers have a team of experts with years of experience in the field.

They have the knowledge and skills needed to identify potential risks and vulnerabilities, and to implement effective solutions to mitigate those risks.

## Cost-effective Security Protection

Outsourcing cybersecurity can be a more cost-effective solution than hiring a full-time cybersecurity team.

The cost of maintaining an in-house cybersecurity team can be significant, particularly for smaller businesses.

By outsourcing, businesses can access the same level of expertise and experience at a lower cost.

## Access to the latest technology

Cybersecurity providers invest in the latest technology and tools to protect their clients from cyber threats.

By outsourcing, businesses can access the latest technology and tools without having to make a significant investment themselves.

## Focus on core business

By outsourcing cybersecurity, businesses can focus on their core activities without worrying about the day-to-day management of cybersecurity.

This allows businesses to be more productive and to focus on what they do best.

## 24/7 monitoring and support

Cybersecurity threats can occur at any time of the day or night.

Cybersecurity providers offer 24/7 monitoring and support, ensuring that businesses are protected around the clock.

# Securing a Free and Open Cyber Space

Securing a free and open cyber space is a shared responsibility that requires collaboration between government, industry, and civil society.

The UK government has been at the forefront of developing cybersecurity policies and initiatives to ensure the safety and security of its citizens.

For example, the UK government launched the CyberFirst programme to develop the next generation of cybersecurity professionals.

We need to work together to develop and implement effective cybersecurity policies, standards, and best practices.

We also need to educate and raise awareness among users about the risks and threats they face in the cyber space, and provide them with the tools and resources they need to protect themselves.

Businesses also have a crucial role to play in securing the cyber space. According to a survey by PwC, 87% of UK CEOs are concerned about cyber threats, but only 33% have an incident response plan in place. This highlights the need for businesses to take proactive measures to protect themselves against cyberattacks.

One of the most effective ways for businesses to take a proactive approach to protect themselves against cyberattacks is to engage with a specialist cyber security services provider.

By doing so, businesses can benefit from the expertise and tooling of experienced professionals without adding unnecessary strain on their internal teams or investing in expensive new technology.

Cyber security service providers offer a range of services, including vulnerability assessments, threat intelligence, and incident response planning, among others.

These services can help businesses identify and mitigate vulnerabilities, detect and respond to threats, and develop proactive strategies to prevent future attacks.

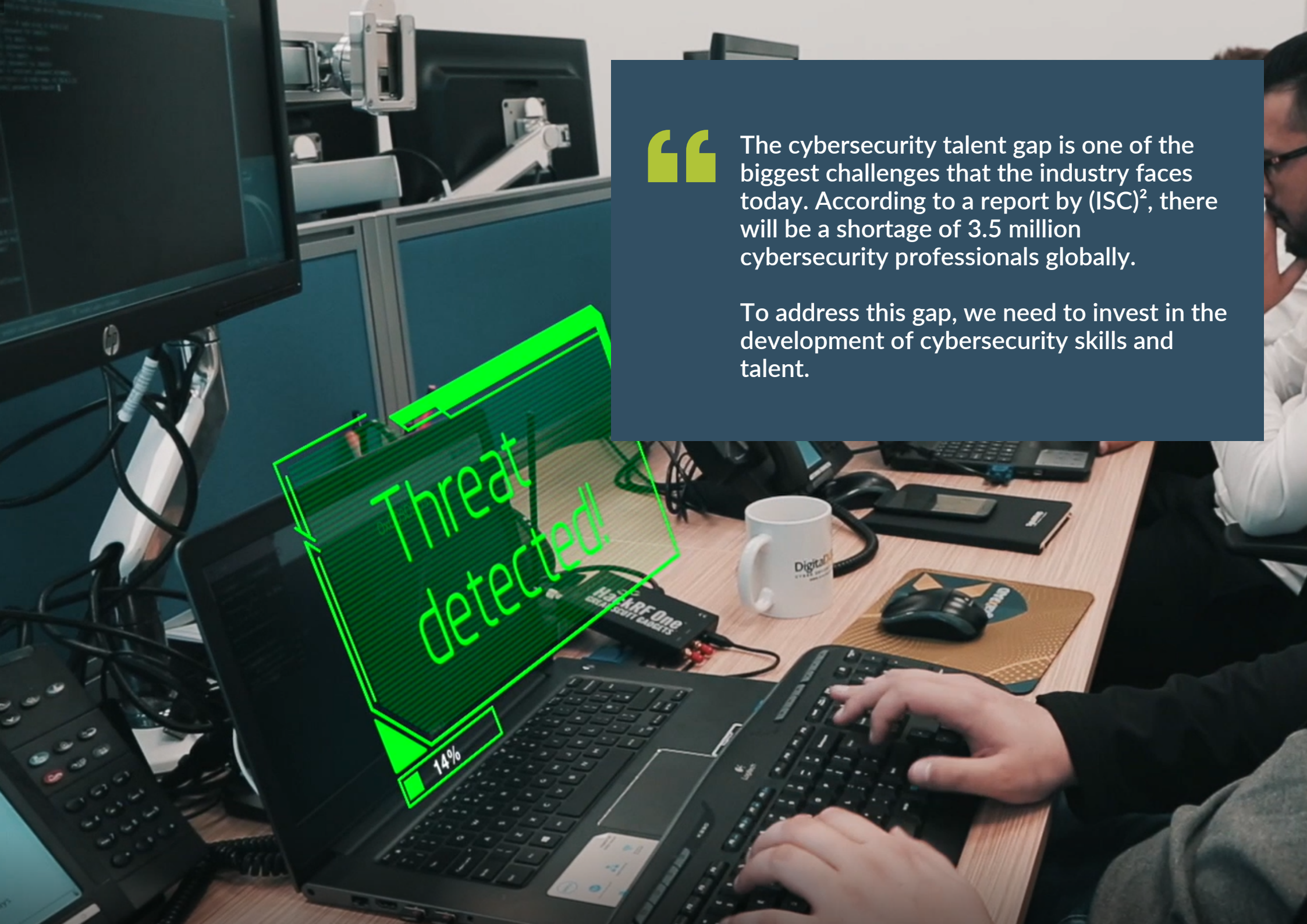
Engaging with a cyber security service provider can also help businesses stay up to date with the latest cybersecurity trends and best practices, as well as comply with industry-specific regulations and standards.

By partnering with a trusted provider, businesses can ensure they have the necessary knowledge, skills, and resources to protect themselves against the evolving threat landscape.

Furthermore, partnering with a cyber security service provider can provide businesses with cost-effective solutions that may be more efficient than building their own internal capabilities.

By outsourcing cyber security services, businesses can save time and money, as well as focus on their core business objectives.

**The Government's Cyber Breaches Survey revealed that 39% of businesses in the UK had suffered a cyberattack during the previous 12 months.**




> The cybersecurity talent gap is one of the biggest challenges that the industry faces today. According to a report by (ISC)², there will be a shortage of 3.5 million cybersecurity professionals globally.
>
> To address this gap, we need to invest in the development of cybersecurity skills and talent.

# Nurturing and Growing Cybersecurity Talent

The UK government has recognised the importance of talent development in cybersecurity and has launched a number of initiatives to address the talent gap.

The National Cyber Security Centre (NCSC) has launched the CyberFirst Girls competition to encourage more young girls to pursue careers in cybersecurity.

To address this gap, we need to invest in the development of cybersecurity skills and talent.

This includes providing training and education to individuals who are interested in pursuing a career in cybersecurity, as well as creating opportunities for existing professionals to upskill and reskill.

We also need to ensure that cybersecurity is an attractive and rewarding career option, and that we provide a supportive and inclusive environment for all cybersecurity professionals.

One way to access and support top cybersecurity talent is by partnering with cybersecurity service providers.

These providers typically employ some of the highest qualified and experienced security professionals in the industry, who are equipped with the latest tools and technologies to address evolving cybersecurity threats.

According to a survey by Deloitte, 71% of cybersecurity professionals prefer to work for service providers due to the opportunity to work on a more varied workload, rather than just focusing on one area of security.

Additionally, 81% of respondents stated that working for a cybersecurity service provider provides more opportunities for career advancement than working in-house.

# Predicting and Mitigating Risks and Vulnerabilities

Predicting and mitigating risks and vulnerabilities is an essential part of cybersecurity.

We need to stay ahead of the threats by continuously monitoring the cyber landscape and identifying potential risks and vulnerabilities.

We also need to develop and implement effective risk management strategies that can mitigate the impact of cyberattacks and other security incidents.

The UK government has launched a number of initiatives to help businesses mitigate cyber risks. For example, the Cyber Assessment Framework to help organisations assess and improve their cybersecurity posture.

However, for organisations to have complete 24/7 threat protection, outsourcing to a cyber security service provider is highly recommended.

These providers offer a range of services that can best support risk mitigation, including Penetration Testing and Vulnerability Scanning.

Penetration testing simulates an attack on an organisation's systems, identifying weaknesses and vulnerabilities that hackers could exploit. Vulnerability scanning, on the other hand, is a non-intrusive method of identifying potential vulnerabilities in an organisation's systems, applications, and networks.

In addition to these services, a Security Operations Centre (SOC) can provide complete 24/7 threat protection.

A SOC is a centralised unit responsible for monitoring, detecting, and responding to security incidents.

They use advanced tools and techniques to identify and investigate potential threats and vulnerabilities, providing real-time threat intelligence and incident response.

By outsourcing to a cyber security service provider, organisations can benefit from the expertise and tooling without adding any additional strain on their internal teams or expensive new technology.

This can help organisations to better mitigate risks and vulnerabilities, ensuring that they remain secure in the ever-evolving cyber landscape.

**Building resilience to cyber threats is a critical component of cybersecurity**

# Building Resilience to Cyber Threats

We need to ensure that we have effective incident response plans in place that can help us to respond quickly and effectively to security incidents.

We also need to conduct regular cybersecurity assessments and audits to identify potential weaknesses and vulnerabilities, and to take proactive measures to address them.

However, building in-house cybersecurity teams and implementing effective cybersecurity measures can be a challenging and expensive process.

According to a report by EY, the cost of building an in-house cybersecurity team now ranges from £1.5 million to £10 million per year, depending on the size and complexity of the organisation.

Furthermore, there is a lack of skilled cybersecurity professionals in the market, making it difficult for businesses to build and maintain effective cybersecurity teams.

This shortage is a major challenge for businesses, as they struggle to find the right talent to build and maintain their cybersecurity infrastructure.

Partnering with a cybersecurity service provider can be a cost-effective solution to building resilience against cyber threats.

Cybersecurity service providers have access to a wide range of skilled professionals and cutting-edge technology, making it easier for businesses to address their cybersecurity needs without the added strain on internal teams or expensive new technology.

Cybersecurity service providers offer a range of services that can help businesses to build resilience against cyber threats, including penetration testing, vulnerability scanning, and security operations centre (SOC) services for complete 24/7 threat protection.

By partnering with a cybersecurity service provider, businesses can benefit from their expertise and tooling, ensuring that they are well-equipped to detect and respond to cyber threats in real-time.

This can help businesses to stay ahead of the threats and build long-term resilience against cyber threats.

> The future of cybersecurity is uncertain, but it is clear that it will play a critical role in ensuring that the digital space remains free, open, and democratic.
>
> The challenges we face will require us to be innovative, proactive, and resilient, and will require collaboration between government, industry, and civil society.

DigitalXRAID
CYBER SECURITY EXPERTS

At DigitalXRAID, we understand the challenges facing businesses in today's rapidly evolving cybersecurity landscape.

Our services are designed to help businesses strengthen their security posture and protect them from cyber attacks.

As a leading provider of cybersecurity services, we offer a range of solutions that can help businesses to identify, assess, and mitigate potential risks and vulnerabilities.

Our services include penetration testing, vulnerability scanning, and incident response planning.

Our flagship service is the CREST Accredited Security Operations Centre (SOC), which can offer 24/7/365 extended detection and response (XDR) protection against cyber attacks.

With a SOC in place however, attacks can be detected and responded to before they become a critical event.

If you're looking into how you can better protect your business, get in touch with us. We have some of the highest qualified security professionals in the country ready to help you take your first step to safeguard your organisation.

DigitalXRAID

CYBER SECURITY EXPERTS

## Need the Best Defence Against Cyber Threats?

## Call us now on 0800 090 3734

info@digitalxraid.com digitalxraid.com

ISO 27001 INFORMATION SECURITY MANAGEMENT

ISO 9001 QUALITY MANAGEMENT

CYBER ESSENTIALS CERTIFIED PLUS

IASME CONSORTIUM

CREST

Assured Service Provider

in association with National Cyber Security Centre

CHECK Penetration Testing