TryHackMe

The World's Cyber Security **Powerhouses**

- Who's **Leading**, Who's **Lagging**?

Introduction

Cyber security is a necessity, with cyber crime growing at an alarming rate with threats sweeping the globe. Over the next three years, experts estimate that cyber crime will cost the world **$10.5 trillion**, equating to a staggering 250% spike in just a decade.

Cyber security around the world differs significantly, emphasising the wide variety of approaches to cyber security defence taken by nations. The global cyber security industry is facing a battle in two aspects. Externally, an increased global threat with no sign of cyber attacks slowing down. Internally, it's battling a continuous shortage of professionals.

In this report, discover how cyber security differs from country to country, the magnitude of cyber crime across the world, and the critical insights of the global cyber security market.

Cyber crime around the world

Cyber crime is a growing concern to countries at all levels of development. However, rates of cyber crime differ widely across the globe due to the evolving cyber crime landscape, resulting in skill gaps and legislation variations.

Less-developed countries are most likely to see the highest rate of cyber crime, while those in more developed nations are more likely to become victims.

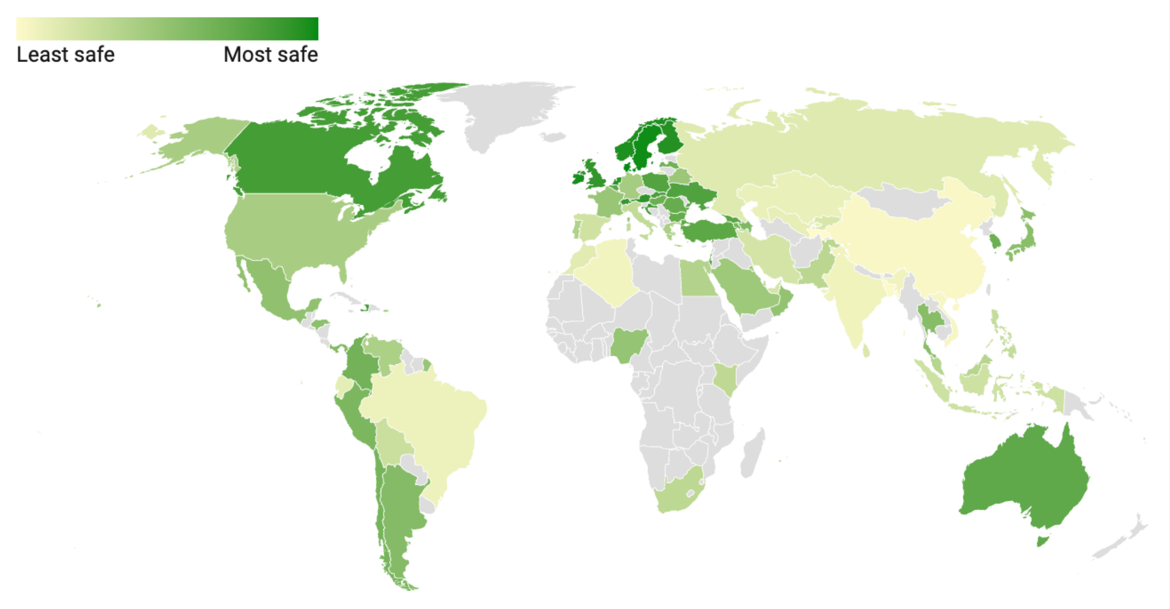
> *“Developed nations have higher incomes, technology, urbanisation, and digitalisation, which are all factors for greater cyber risk.”*
>
> *NordVPN*

Cyber Security around the world

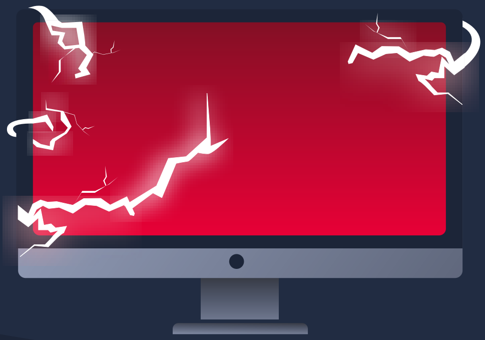
Europe has the highest adoption rate (91%) of enacting cyber crime legislation, while Africa has the lowest (72%). In total, 156 (80%) countries around the globe have passed legislation. An astonishing 13% of countries have no legislation, with no intention of introducing legislation soon.

Cyber security is, and should always be a global concern. With that in mind, many regions worldwide fail to address these risks, leading to an increasingly alarming rate of cyber attacks.

Analysing cyber security around the world enables patterns to be recognised in areas where cyber crime is more prevalent. Whilst most affluent countries may be hit, less-developed countries are more likely to suffer the long-term irreversible damage of attacks due to a lack of defences. Those countries with leading laws and processes should be benchmarked as leaders in the industry.



Areas with the highest rate of cyber crime



Tajikistan tops the list as the least cyber secure country in the world, with a lack of measures and legal enforcement. With the highest percentage of malware attacks, ransomware trojans, and attacks by cryptominers, Tajikistan is significantly vulnerable to cyber threats from around the globe.

With minimal legal measures, the lack of technical support, and a spike in sales of disreputable mobile devices and app stores, Tajikistan nationals are warned to take appropriate measures to protect themselves.

Uzbekistan, Kazakhstan, Kyrgyzstan, Cambodia, Honduras, Bolivia, Mongolia, Algeria, Zimbabwe, Nicaragua, and Bosnia-Herzegovina follow closely behind Tajikistan as having some of the highest cyber crime rates in the world.

Areas with the lowest rate of cyber crime

While countries across the globe are facing increasingly sophisticated cyber attacks, Denmark leads the global race in cyber security with the lowest rate of cyber crime in the world.

Following a devastating cyber attack in 2016 which saw hackers gain access to email accounts of select members of the Danish Defence, Denmark now holds the title of the most cyber secure country in the world - closely followed by Germany, the United States, Norway, the UK, Canada, Sweden, and Australia.

Based on the percentage of malware-infected devices in the country, Denmark continuously ranks incredibly well, placed in the top three when identifying the lowest scoring countries for:

Mobile devices

Mobiles infected with malware

1.06% – Finland
1.15% – Ukraine
1.33% – Denmark

Users attacked by mobile ransomware trojans

0.00% – Denmark, Argentina, Japan, Austria, Belarus, Turkey, Chile, Colombia, Ecuador, France, Hungary, Haiti, Greece, Australia, Latvia, Peru, Tajikistan, Brazil, and Venezuela

Mobile banking

Users attacked by mobile banking trojans

0.00% – Denmark, Egypt, Algeria, Mexico, Argentina, Haiti, Hungary, Ireland, Nigeria, and Thailand

Users attacked by banking malware

0.03% – Ecuador
0.05% – Bolivia
0.10% – Denmark, Ireland, and Panama

Computing

Computers infected with at least one web-based malware attack

0.48% – Haiti
1.33% – Denmark
1.35% – Ireland

Computers facing at least one local malware attack

2.83% – Denmark
3.34% – Sweden
3.49% – Ireland

Ransomware trojans

Users attacked by ransomware trojans

0.02% – Denmark
0.03% – Sweden
0.04% – Ireland and Romania

Cryptomining

Share of attacks by cryptominers

0.05% – Haiti
0.11% – Denmark and Japan
0.12% – Germany

Phishing

Computers attacked by phishing

1.94% – Haiti
3.26% – Denmark
3.35% – Sweden

Global cyber security threats

Though there is a vast difference between cyber security and threats worldwide, one key recurring factor is the type of global cyber threats we are seeing, partly due to the world's shift to remote working.

30,000	623 million	10%
websites are hacked every day	ransomware attacks took place in the last year	of all breaches include malware

Globally, 30,000 websites are hacked daily. Analysts exploring these annual worldwide cyber trends predict the United States will become the target of over 50% of worldwide cyber crime attacks in the next five years.

Ransomware is the biggest global cyber security issue, with around 623 million ransomware attacks worldwide in the last year alone.

As the most prominent malware threat online today, ransomware is part of 10% of all breaches around the globe, with the potential to significantly affect entire societies and economies. Ransomware is, therefore, the most detrimental threat facing businesses and individuals today.

Since the first documented ransomware attack in 1989, ransomware varieties have evolved in their capabilities for coercing users, evading detection, and encrypting files.

New-age ransomware utilises sophisticated encryption algorithms, such as RSA encryption, alongside advanced development techniques intending to make each attack more challenging to prevent and more damaging to ransomware victims. While early ransomware was configured with manually-written encryption code, today's attackers are exploiting off-the-shelf libraries of ransomware code, making it easier and quicker for attackers to widely distribute ransomware attacks.

Ransomware attackers are leveraging a combination of human error and increasingly sophisticated attacks that are significantly harder to crack, including the technique of using spear-phishing campaigns to distribute attacks.

With financial gain being a core goal for hackers, analysts predict ransomware becoming the most dominant cyber threat to businesses. Even today, businesses suffer ransomware attacks every 40 seconds. As a result, ensuring preventative measures in your organisation is essential.

Global ransomware attacks

WannaCry

The WannaCry attack was estimated to have affected approximately 230,000 devices in over 150 countries. As a result of the ransomware attack, over a third of NHS hospital trusts in the **United Kingdom** were infected with the software, which was said to have cost them over £92m.

Ryuk

Ryuk made over £500,000 in just a fortnight by targeting organisations globally, compromising governments, healthcare, manufacturing, academia and technology organisations. Ryuk has commonly distributed through Emotet or TrickBot malware, although it is not yet clear where Ryuk originates from. While organisations around the world have fallen victim to Ryuk, the **United States** became a primary target.

NotPetya

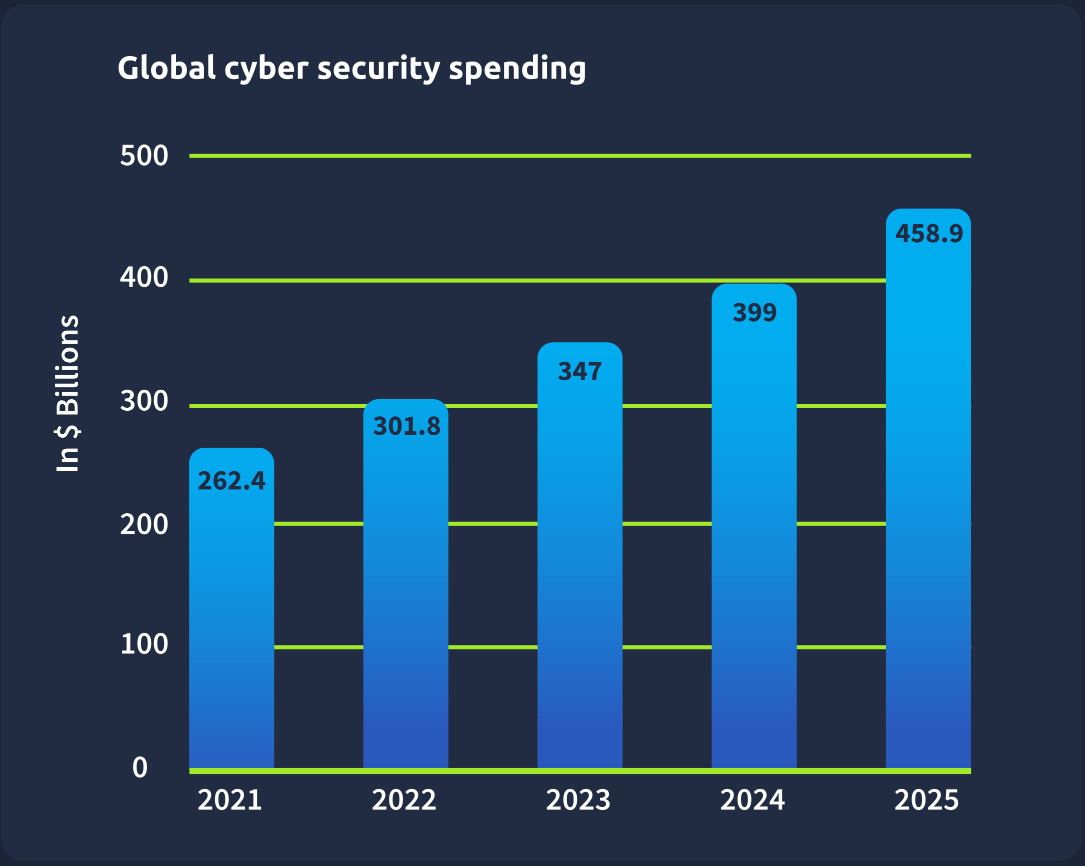
In early 2017, NotPetya malware rapidly spread across **Europe**, causing an estimated $10 million in damages to industries. The attackers hijacked the MeDoc update servers, before gathering information from the servers and developing a false update patch distributed to all computers using the MeDoc software. **Ukraine** was mostly impacted by the ransomware attack which swamped the websites of Ukrainian organisations, including banks, ministries, newspapers and electricity firms. NotPetya has been described as one of the biggest and most devastating ransomware attacks in history.

Sodinokibi (REvil)

Sodinokibi ransomware is notorious for its sophisticated evasion capacity and ability to remain undetected by anti-virus engines. In recent cases, the ransomware demanded $50 million for the decryption key to unlock their systems. Sodinokibi is ransomware as a service (RaaS), meaning that one group writes and develops the code, while another group distributes it. The ransomware attacked targets across the world. In addition, it’s estimated that 80% of all Sodinokibi infections were in **Ukraine**, with **Germany** second hardest hit with around 9%. Other affected countries include the **United Kingdom**, **Japan**, **Italy**, and **Spain**.

Global cyber security spending

In the digital age, cyber security is no longer a luxury but a necessity that can influence the survival and success of your business. Cyber security should be seen as an investment, with cyber crime estimated to cost the world $10.5 trillion annually with world cyber security spending reaching $458.9 billion, by 2025.



While cyber security has become an ever-relevant topic, insufficient allocations for cyber security spending has become a problem in almost every industry. While many organisations will limit cyber security spending in line with budgets, there is never enough you can spend on cyber security to protect your business.

> *“ Today, cyber security is often an invisible part of our life which we take for granted, but we owe it almost everything we have achieved as a civilization. ”*
>
> *Vitaly Kamluk,*
> *Head of Asia-Pacific Research & Analysis Team at Kaspersky*

As cyber threats continue to advance, it is vital to evaluate the cyber security spending trends of your industry and allocate a higher budget to protecting your business and its data. With that in mind, how and where you invest cyber security spending is crucial.

Building an efficient cyber security budget should be a process with thoughtful consideration of multiple factors and outside influences. The intended level of spending should align with your chosen level of risk and desired level of protection.

All organisations throughout the world are vulnerable to cyber attacks, and as such, need to be aware of their cyber security landscape. A cyber attack can completely inhibit any organisation, resulting in loss of time, money, and a detrimental reputation. It is absolutely vital to invest in the right infrastructure and teams to help protect you from attacks.

TryHackMe is here to make that as accessible and fun for your team as possible, with training pathways allowing cyber security teams to stay on top of new threats and advances in the industry.

The global cyber security career market

The cyber security industry is facing a battle in two aspects. Externally, an increased global threat with no sign of cyber attacks slowing down. Internally, it's battling a continuous shortage of professionals.

3.5 million
cyber security professionals are needed worldwide to meet growing demand.

Demand for trained security professionals remains at an all-time high as the cyber security industry is inevitably **facing a major shortage of cyber security skills.** The global cyber security workforce is required to grow 65% to effectively defend organisations' critical assets. Across all 12 European countries, at least 60,000 additional cyber professionals are needed to meet the demand, with an estimated shortage of 3.5 million cyber security professionals worldwide.

Technical advances now underpin human progress across the globe. Yet, without training and hiring the talent to secure these innovations, industries are unable to protect against cyber threats. As a critical component of other functioning industries, cyber security professionals should be considered as essential as any other key sector, specifically with incident response and threat management as the two most crucial skills needed globally.

As a result of the global cyber security skills shortage, cyber security salaries are growing at their fastest rate in history. In the last year alone, the average cyber security salary soared by a huge 12%. In addition, employers within the field are advised to keep employee turnover as low as possible.

While the **cyber security job market** differs around the world, countries are experiencing a record-high number of cyber security jobs available, with very few candidates available to meet these positions.

With the industry boom and shortage of cyber security professionals, there has never been a better time to **upskill your team** through short, gamified, real-world labs alongside a range of learning resources.

Singapore

Singapore maintains the highest number of cyber security job openings due to the rapid rise in cyber crime and scams in Singapore, alongside a major shift in adopting a more proactive approach to cyber threats.

The cyber skill gap in Singapore has left businesses "inundated" by an endless stream of cyber attacks. When interviewing business owners, 80% said security breaches in the past 12 months led to losses of up to 10% of their organisation's revenue.

> *“ Threats are evolving so fast, with 62% of cybersecurity professionals in Singapore finding it challenging to keep up, and organisations facing an average of 54 security incidents a day. ”*
>
> *Eileen Yu,*
> *Senior Contributing Editor at Innovation*

With the rapid rise in cyber crime, phishing schemes, and cyber scams in Singapore, we have seen the increasing need for Cyber Security Analysts.

Australia

Surges in cyber crime, ransom attacks, data theft and fraudulent attacks have left Australia in an unfortunate cyber security standing. It’s estimated that Australia will be short of 30,000 cyber professionals over the next four years - four times the number that has been previously calculated. Currently, the Australian cyber security workforce stands at 68,400 professionals.

Like most of the world, Australia faces a fight for talent from more developed markets in the US, UK and Canada. The cyber security gender gap is more prevalent in Australia, with only 21% of women making up the workforce, compared to a higher global average of 25%.

Poland

The threat of tech skills shortage is looming large within the European Union, with Poland reporting a 36% increase in cyber security professionals in the last year alone.

The Polish National Cyber Security Strategy aims to increase the level of resilience to cyber threats and protection of information in the public, military and private sectors, as well as promoting knowledge and good practices to enable the citizens to better protect information. To achieve this, additional investment and a surge in skilled cyber professionals are required.

The cyber security gender disparity is more severe in Poland, with only 13% of females making up the cyber security workforce - 12% lower than the global average.

Canada

The shortage of talent demand has left Canada facing a shortfall of 25,000 workers in the cyber security sector, resulting in businesses, education institutions, and the Canadian Government all taking steps to close the Canada cyber talent gap.

A core issue in attracting and retaining talent is the salaries and incentives failing to keep up with market rates, which are continually inflated due to the lack of supply to meet demand. On a positive note, the cyber security gender gap is less prominent in Canada, with females making up 29% of the cyber security workforce - 4% higher than the global average.

Educational institutions across Canada recognise the vital role in diminishing the cyber security skill gap in Canada, with an increased need to develop cyber security talent. Governments around the world are expected to increase their spending on cyber security, and Canada is among them.

Germany

The cyber crime threat in Germany is said to be higher than ever before, with 71% of German cyber security professionals admitting that attacks increased due to employees working remotely.

With a cyber security skills shortage also evident in Germany, local enterprises are overwhelmed with the lack of qualified professionals, and are even turning to managed service providers and third parties to assist with their security needs.

German enterprises are hoping to increase the supply of skilled workers through training and upskilling to improve their cyber security.

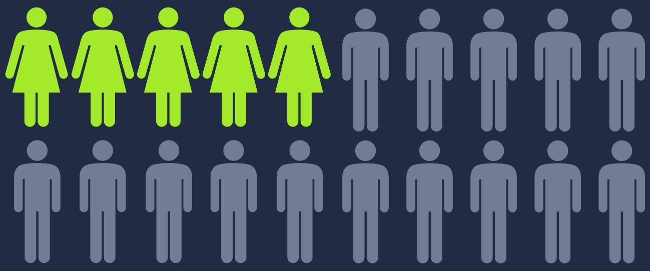
Preparing a new generation of cyber professionals

The way forward is to make all governments, businesses and individuals part of the solution and empower a new generation of cyber-savvy individuals.

Alongside international collaboration, societal awareness, cooperation between public and private sectors, and high-level commitment from businesses and governments, preparing a new generation of cyber professionals is crucial in combatting cyber security risks.

Best-in-class countries that lead the race against cyber crime have built a stronger capacity across society through training, sponsoring and supporting young people interested in front-line cyber defence roles. Mentoring programmes, practical hands-on training, regional cyber initiatives, and cyber security work placements are all long-term solutions that can open the doors to careers in cyber and defending the global battle.

The cyber security gender gap is another hurdle in the industry, with a gender imbalance across the globe. Women account for just 25% of the cyber security workforce, highlighting the need to bring underrepresented groups into the field.



> *“The education of the next generation of cyber experts must start now, including all those that have historically been limited to be part of this defence of our ways of life. We need women in cyber at all levels and tasks.”*
>
> *Ian R. McAndrew, PhD*

Empowering women in cyber and diversifying cyber teams should be a global interest, with women considerably underrepresented in the sector. Countries with a low representation of women in the field should shift efforts into exposing teenage women, or younger, to cyber security as a viable career option.

Following in Denmark’s footsteps

How did Denmark achieve the title of the most cyber secure country in the world after a critical data leak?

With the data leak considered a serious threat to the nation's security, the Danish government has launched a number of initiatives for developing Denmark towards becoming stronger and more digitally secure, promoting the importance of cyber security measures to individuals and businesses through campaigns.

> “ *In recent years, the Danish government has launched a number of new initiatives for developing Denmark towards becoming stronger and more digitally secure.* ”
>
> *Ministry of Foreign Affairs of Denmark*
> *(Invest in Denmark)*

The introduction of widespread implementation of two-factor authentication, better-developed banking apps, strict legislation and numerous laws promoting cyber security have resulted in Denmark maintaining its position as one of the most digitised countries in the world. Other factors include the wide-ranging digitisation of public services, a technologically proficient population, and businesses implementing new technology at a fast pace.

Established as a benchmark for the industry, Denmark continues to engage and invest in cyber security initiatives, and is no longer perceived as a high-profile cyber target.

Denmark’s cyber security initiatives

The Danish government agrees with a majority in Parliament to strengthen Denmark’s cyber defence by DKK 500 million through the implementation of the political agreement on the cyber reserve.

> “ *A more concentrated effort is needed to keep up with and be at the forefront to meet developments in threats and digital vulnerabilities. This is why the Government is now launching a new Danish National Strategy for Cyber and Information Security 2022-2024.* ”
>
> *The Danish Ministry of Finance*

The Danish National Strategy for Cyber and Information Security continues to strengthen Denmark’s cyber and security standing with new initiatives tying overall efforts together. With this in mind, the Danish Government will be allocating a total of DKK 270 million to 34 new key Initiatives. These cyber security initiatives are designed to drive Denmark to become more digitally secure.

Robust protection of vital societal functions

Maintaining vital societal functions and economic activity in a crisis where critical ICT infrastructure is non-functional for a short or longer period. Businesses and government agencies must have a sufficient level of security to act on short notice in the event of serious cyber incidents.

Increased level of skills and management commitment

Cyber and information security are to be embedded in top management, and skills must be strengthened. Citizens, businesses and government agencies should have awareness of how to protect themselves and remain digitally safe. In relation to Denmark's cyber skills shortage, the demand for security skills must be accommodated through training and building stronger capacity across society.

Strengthening of the cooperation between the public and private sector

Strengthening cooperation across sectors, sharing knowledge, and learning from each other is vital to achieving a high cyber and information security level. Businesses and government agencies should cooperate more closely, supported by highly specialised consultancy through centralised coordination.

Active participation in the international fight against the cyber threat

International cooperation in the EU, UN, NATO and like-minded countries must be strengthened within the organisations that can develop norms and define standards for cyberspace if the underlying causes of cyber attacks are to be fought. Denmark must actively contribute, making it difficult and consequential to conduct cyber attacks against Denmark.

Building a global response to cyber security risks

To create a cyber-secure world, we must be globally integrated and create a global response to cyber security risks. Local resources will not be enough, therefore countries must coordinate their efforts in a collaborative approach that aids low and middle-income countries to become more resilient in respect of cyber attacks and responses.

> *“Like pandemics, income inequality and extreme weather caused by climate change, cyber security is a global problem. But while there is some degree of global cooperation for addressing the first three issues, to date, there hasn’t been that same level of cooperation around cyber security. ”*
>
> *Kevin Lynch,*
> *Forbes Councils Member*

Creating a global cyber security strategy should be the first step in making progress towards becoming a cyber-secure world. Developing a greater understanding of the risks and how they may impact financial stability is crucial, including the nature of threats and the impact of successful attacks.

In creating a global strategy, countries across the world must improve collaboration on threat intelligence, incident reporting and best practices in resilience and response, with seamless communication for greater consistency throughout nations. Regulatory approaches need to achieve greater consistency, with different standards and regulations creating gaps and weaknesses in less-developed countries.

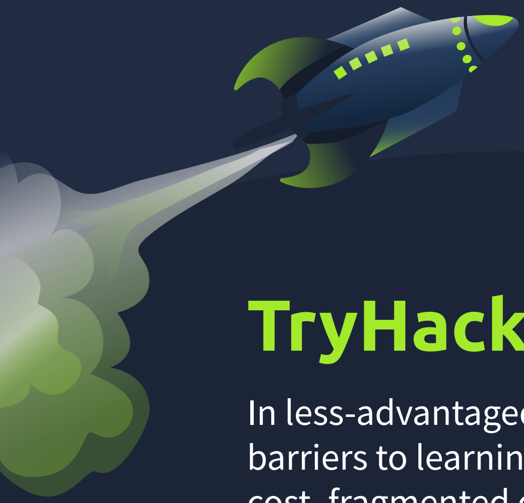
> “ *To act fast, we must share threat information in near real-time. Cyber crime has no borders. In a world that is so deeply interconnected by digital technology, cyber security and global security are the same thing. No single organisation, public or private, can have a complete view of the entire cyber landscape.* ”
>
> *Ken Xie,*
> *Fortinet*

As governments develop cyber security laws to prevent, investigate, and take action against cyber crimes, they should focus on robust substantive and procedural cyber security laws. Governments alone are unable to improve the cyber security of their entire country, without the collaboration of businesses and individuals. Best-in-class governments have higher opportunities to thrive, with advanced cyber security capabilities and cyber awareness in individuals.

Countries need to be ready for attacks, knowing that crisis preparation and response protocols should be put in place ahead of inevitable attacks for a smoother recovery. Crisis exercises have become crucial in building resilience and the ability to respond.

Countries focusing their efforts on core cyber security strategies may be in a better position to prevent cyber attacks, mitigate their damage, and better protect their businesses, individuals, and critical infrastructure.

> “ *Governments need to decide which aspects of cyber security they want to legislate and which aspects they want to provide guidance on without necessarily imposing any legal penalties. One good option while developing national cyber security laws is to embrace the guidelines laid out by the Budapest Convention—an international treaty governing cyber laws agreed upon by more than 60 countries.* ”



TryHackMe’s mission

In less-advantaged countries where cyber crime is rife, common barriers to learning and progressing in cyber security include the high cost, fragmented quality of learning material and experience and more. Improved cyber security education can reduce global cyber risk by creating a more secure cyber culture across the globe.

TryHackMe is the fastest growing, community-first cyber training company, and we want to help students and cyber professionals learn (and upskill) in cyber security to meet the global pressure. Our mission is to make it easier for people to break into and upskill in cyber security, with an emphasis on closing the cyber skill gap.

We use virtual rooms, allowing users to deploy training environments and learn with a hands-on approach. TryHackMe aims to remove as many of these barriers as possible, through an affordable subscription cost and structured learning paths aligned to cyber security careers.

Cyber security training should be as engaging, real-world and beginner-friendly as possible, which is why TryHackMe users of any skill level can sign up and start learning how to become an ethical hacker, penetration tester or cyber security analyst.