
# Cybersecurity Talent Crisis

## Today and Tomorrow

**Codrut Andrei** 7/5/22 https://www.linkedin.com/in/codrutandrei/

# Contents

# EXECUTIVE SUMMARY

***When there will be no electricity to power our houses, no gas to prepare our food, no critical infrastructure to support our lives, it is going to be too late to ask ourselves:***

***"Have we done everything to prevent this?"***

This is going to be our baseline for this report, a future scenario that looks like the digital doomsday and the end of the normal life that we are so used with.

While it seems that there is a small chance this could happen, it already did. Think of the Ukraine and U.S. power grid hacks, the Colonial Pipeline, WannaCry, SolarWinds, NotPetya and so on. Remember when we moved remote and the beginning of the pandemic, all of us were under attack, our healthcare system was down multiple times, and our basic human rights were monetized by the malicious actors.

From $3 trillion USD in 2015, $6 trillion in 2021 and potentially reaching $10.5 trillion by 2025, cybercrime became the 3rd largest economy in the world after U.S and China. Due to the year over year increase, nation-state sponsored attacks, organized crime cyber activities and an increased attack surface, cybercrime will soon rival mother nature itself.

The threat landscape is evolving and finding solutions to close the talent gap along with strengthening our defenses and make strategic investments in cybersecurity is the only way to keep up with all the changes that are happening around us.

The cybersecurity talent crisis is the shortfall of capable workforce to oversee cybersecurity tasks and goals. This is not just a cybersecurity problem but also an issue that affects our economic and social development, national security, our privacy, and basic needs.

There is not a single and simple explanation of what caused the talent shortage, but the main ones might be attributed to the pandemic and digitalization on one hand and education and training systems on the other.

The pandemic and digitalization are a recent addition and just short-circuited and worsened the crisis while education and training systems are around for a long time.

This research paper will try to answer to some of the following questions:

1. Does the talent gap exist or is just a market exaggeration?
2. How have we got here?
3. Is there any real impact?
4. What are the most common problems that we see today?
5. How can we close the talent gap?

We see an overall dissatisfaction with compensation, development opportunities and culture and those playing a significant role with either joining or leaving a company.

One of the phenomena we see in the market today is organizations trying to buy the talent but not making any investments for the future. We seek people with many years of experience, already certified that can bring value from day 1, and there is nothing wrong with that, but we are quite missing the fact that we also need to build the next generation of cyber professionals.

## "Stop chasing 'All Stars' for the short-term gain and develop your team for years of success"[1]

While going through the available public data on the subject one of the most interesting facts is around how we measure the talent gap, you will find different numbers and the same applies to, average total costs of data breaches and any other statistic or measurement.

Another problem that is flagged by these reports is that while we chase technical skills, we understood that in today's environment these are not enough to be successful. We need to make investments into human skills (soft skills), add these into our technical trainings, academic curricula, and overall talk more about the importance of having these critical skills. We need our cyber experts to get involved and give a little bit of their time and start acting as mentors and coaches for the next generation of cyber professionals and most importantly we need to seek people that are willing to learn and want to get into this field.

There are papers and voices talking about the young generation taking a turn to the dark side and instead of contributing to their community and society and use their skills to harm others.

[1] (ISC)², 2021 (ISC)² Cybersecurity Career Pursuers Study, https://cloud.connect.isc2.org/career-pursuers-report

We must think about offering them a safe place to practice their skills, feed their curiosity and teach them ethics and what is the moral way to use their intellect.

As a community we need to invite more people in the field, diversify, bring new talent and innovative ideas and start working together to remediate this problem as we need our next generation to protect us and our way of life.

Statistics can be biased but can still tell a story and at least can point in a certain direction. It is not as relevant if 90% or 40% complain about burnout, if we lose $5M or $1M in a data breach, what matters is that people are talking about these and what is most important – what we are going to do about it.

This paper is based on my research on the topic and will reflect the public data shared as well as my professional opinions on the issues and personal suggestions to close the gap. I do not consider it an academic paper but a tool to understand how we got here, where we are and what steps can we take to get closer to a more secure tomorrow.

The time to ACT is NOW!

# INTRODUCTION

The goals for this paper are:

1. Raise Awareness
2. Shift Perspectives
3. Supply guidance and options to close the talent gap

## Raising Awareness

Like with many other things we start paying attention to a problem only when it gets worse. Like ransomware that is around since 1989, the talent gap has been reported for at least a decade.

One of the first warnings came in 2010 with a report called “A Human Capital Crisis in Cybersecurity” by the Center for Strategic & International Studies. Then, in 2016 “Hacking the Skills Shortage” report from McAfee was mentioning that 82% of the survey respondents reported a shortage of cybersecurity skills. The existing data clearly shows that little improvements were made over the decade and today the number is close to 60% of the organizations are affected by this problem.

According to (ISC)² 2021 Cybersecurity Workforce Study, the estimate for the supply-demand cybersecurity workforce gap is close to 4.2 million with a 700,000-increase year over year. Another professional association puts the number close to 3 million, but what is certain is that we have millions of unfilled jobs for the cybersecurity domain. This comes with a multitude of problems, and some will be covered by this paper. We must do more research on this topic and more people to talk about it to understand how far and deep this goes.

According to CyberSeek, in U.S. alone there are more the 100,000 job openings that require a CISSP certification but nationwide there are just over 90,000 CISSPs (Certified Information Systems Security Professionals). The other example is even more eye-opening with 40,000 jobs requiring the CISM certification and just 17,000 CISMs (Certified Information Security Managers).

Yes, this is a known problem for a long time and the recent development is that now governments, industries, and organizations acknowledge what is happening because every one of them are affected.

As more experts are looking into this problem and more people are talking about it, we seem to understand more about the size, shape, and form. What started as a recruiting problem slowly evolved into a pandemic, for which, there is no vaccine at this point.

There are multiple dimensions of the problem, and this paper will be a best effort to cover as many as possible. This problem, as well as cybersecurity and technology are constantly changing, only the issues stay the same.

What we acknowledged, and this is a good start, is that our education systems curricula are not up to date enough to prepare the next generation of cybersecurity professionals. Fresh graduates are not ready for entry-level jobs as they are not equipped with the necessary technical skills and more worryingly not even with the human skills. Some of the latest literature talking about this subject is reporting that analytical and critical thinking along with communication are skills missing from people that just finished higher education. This is a frightening thought, knowing the time and financial investment needed for a bachelor or master's degree but not being prepared for a first time job interview.

## The question that we must ask ourselves: Why do we still ask for a bachelor's degree for entry-level jobs?

Data highlighted in this paper is publicly available to everyone. ISACA, Hays, Gartner, (ISC)², ESG just to name a few of the professional associations that released papers on this subject and are the most used and quoted resources in this paper along with others.

Today, at least 60% of the interviewed organizations are reporting this issue, the number is probably much higher considering the scope of the surveys and the fact that the talent gap has multiple sub-issues.

What is most important to remember: this is affecting economic and social development, national security, our privacy, and our basic human rights.

## Shifting Perspectives

We have always looked at the talent gap as a cybersecurity problem but what if we look at this from a different angle? What if we look at the problem through business lens?

Questions to ask ourselves:

1. What if we would treat our cybersecurity professionals as we treat our customers?
2. What if we would look at this as a customer problem?
3. What would we do if our customers would leave for the competition?

If we do not have enough professionals to protect our business, then the talent gap is a business problem that needs a business approach. If we would apply the same tools then we would at once do a SWOT [Strengths, Weaknesses, Opportunities and Threats], PEST [Political, Economic, Social and Technological] and a Gap Analysis. We would put that into a Strategy Map and then Implement those new goals. But we are not doing that.

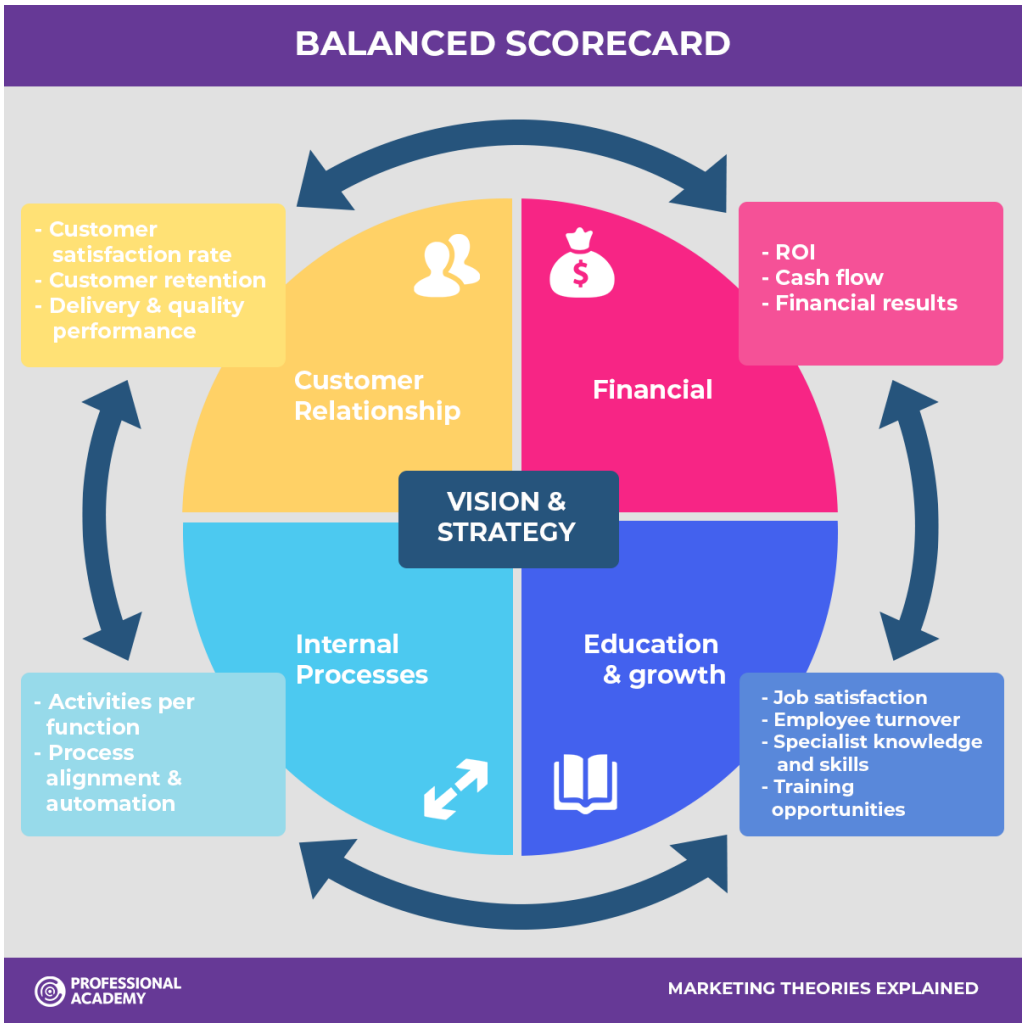
As security professionals we cannot articulate clearly how security is protecting the business and what we are doing to help generate revenue. We must take that responsibility, learn the language if we want to be equal partners, otherwise, we will be kept in the 'Security as a Cost Center' bubble.

***Clar Rosso (ISC)² CEO "As a result of not being fully staffed, systems are being misconfigured. There is not enough time for proper risk assessment and management. Organizations are slow to patch critical systems."***

# THE BALANCED SCORECARD

In this chapter we will look at the existing public data, share the statistics, point out the problems and propose solutions.

To add to our business tools suite, next to SWOT, PEST, and Gap Analysis, we will use the Balanced Scorecard to highlight that the mission, vision and success of any organization is based on the perspective of four different areas. It also tells how efficient we are running our business and if the goals are being met.




Credit: https://www.professionalacademy.com/blogs/marketing-theories-balanced-scorecard/

The Balanced Scorecard has four major areas, as shown above and below you can find the summary of the relation to what we are going to cover:

1. Customer Relationship / Customer [dis]Satisfaction
2. Education and Growth / Learning & Development
3. Internal Processes / Family Affairs
4. Financial / Financial Outcome

## Customer [dis]Satisfaction

I will point out again some of the questions that we have to ask ourselves to understand the data and start thinking and shifting our mindset when we look at the problem. Every time when you see customer think cybersecurity professionals.

1. What if we would treat our cybersecurity professionals as we treat our customers?
2. What if we would look at this as a customer problem?
3. What would we do if our customers would leave for the competition?

Statistics

- **[76%]** Say is extremely/somewhat difficult to hire cyber professionals[2]
- **[62%]** Complained about increased workload[3]
- **[38%]** Mentioned the lack of competitive compensation[4]
- **[38%]** Said that the talent shortage led to burnout and employee attrition[5]
    - **[73%]** of the respondents say that workers have resigned, citing burnout[6]
- **[38%]** Reported that new jobs remained open for months[7]

**INCREASED WORKLOAD AND BURNOUT FOR EMPLOYEES**. What we have seen in the past years, especially with and after the pandemic, is a common theme among cybersecurity professionals, but we also

[2] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V
[3] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V
[4] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V
[5] Hays, Cyber Security Talent Report Addressing the Skills Gap, 2021
[6] HelpNet Security, https://www.helpnetsecurity.com/2022/04/13/modern-enterprise-security-issues/
[7] Hays, Cyber Security Talent Report Addressing the Skills Gap, 2021

see that this phenomenon is starting to alienate cyber people and leaving for different industries and/or taking sabbaticals.

- **[76%]** of respondents say their team members have been forced to take on responsibilities they are not ready for, and **70%** say that the resulting increase in their workload has led them to consider looking for a new role[8]

This looks like a domino effect: we open jobs that we cannot fill, we overwork our employees who are taking all the added workload, which leads to burnout and sloppy decisions that affect our security posture by deploying unsecured and unpatched servers, untested applications, or not doing basic cybersecurity hygiene.

Cybersecurity people are like firefighters all day long, whether we like it or not, the main difference is that we only carry the burden and not the pride of helping the community or our organization.

*"When someone considers a career in a 'helping' profession their thoughts naturally turn to doctors, nurses, teachers, and first responders like police officers or emergency medical technicians. These people devote their lives to helping to keep the world safe and healthy. And although a career in cybersecurity might not be the first job to come to mind, cybersecurity professionals protect the digital world from cybercrime much the same way that police officers protect neighborhoods."* Sandra Wheathley Smerson, Senior Vice President, Threat Intelligence, Marketing and Influencer Communications, Fortinet Inc.

Finding people is just part of the problem, the other side of it is retention. There is a direct correlation between the talent gap and the ability to defend an organization:

- **[68%]** of those who experienced more cyberattacks say they are somewhat or significantly understaffed[9]
- **[68%]** of respondents say that talent shortages directly led to the failure of one or more projects/initiatives[10]
- **[63%]** of those who experienced more cyberattacks say they have difficulties keeping qualified cybersecurity professionals[11]

Understanding the funding limitations and the talent shortage today but also understanding the non-financial factors affecting the recruitment process will help us understand the size of the problem and why this can become a global crisis.

[8] HelpNet Security, https://www.helpnetsecurity.com/2022/04/13/modern-enterprise-security-issues/
[9] ISACA, State of Cybersecurity 2021 Survey
[10] HelpNet Security, https://www.helpnetsecurity.com/2022/04/13/modern-enterprise-security-issues/
[11] ISACA, State of Cybersecurity 2021 Survey

Through the business lens:

- High Churn Rate means Low income and unhappy shareholders
- Our offerings are not competitive enough and our existing customers leave and join the competition
- We would apply MTTR, MTBF or SLAs to measure our processes and to improve

Improving Customer Satisfaction

The first keyword in our attempt to close the talent gap is **RETENTION**. Keeping existing cyber professionals in our organizations is critical to long term planning. We can address that by understanding the existing shared data and the gap in between.

- Competitive Compensation
- Capacity Planning
- Work-life balance, wellness programs and work from home to address stress and burnout
- Rewriting Job Descriptions (JDs)

While the first three bullets include a financial part and might be harder to implement, the fourth it is in our control to make it better. We have all seen those entry-level jobs requiring many years of experience in the field and fancy certifications and that is an aspect of the problem that we really need to address. Recruiting managers must think it through and put on paper the skills and abilities they need in the team. I am not saying to drop higher education, certification or experience from the JDs but adjust that to the organizational needs and financial compensation for the work done.

For most organizations, talent is the single biggest overhead expense and the biggest competitive advantage[12]. With many companies having digitalization as a priority and with the same pool to recruit from, hiring is getting harder and harder.

**"71% of recruiting organizations recruit for more specialized roles than they did five years ago[13]"**

[12] Gartner for HR, Analytics-Driven Talent Strategy, 23 May 2019, https://www.gartner.com/en/documents/3920415

[13] Gartner for HR, Analytics-Driven Talent Strategy, 23 May 2019, https://www.gartner.com/en/documents/3920415

We see (HR) Human Resources becoming more Agile to understand the current needs and evolving skills by analyzing the talent supply, competition and (WFH) Work From Home trend, geo-location.

Another trend that was seen - branding as a tactic to attract candidates and use of employees as ambassadors to spread the message.

HR tactics and strategies alone will not be as successful as intended without hiring managers playing a role in it. With so many changes and new needs to help organizations stay competitive, hiring managers can play a critical role to help HR find the best talent on the market or collaborate and find re-skilling strategies. Helping recruiters by explaining what you are looking for in terms of profile and skills, helping with keywords that will help easily find candidates, and working together to re-write the job descriptions.

***"Employee expectations are changing, and we will need to define productivity much more broadly – inclusive of collaboration, learning, and wellbeing to drive career advancement for every worker"*** *Satya Nadella, CEO at Microsoft*

Question to ask ourselves: How much money are we losing with hiring and replacing talent?

## Learning & Development

While the 'Customer [dis]Satisfaction' section focused more on the talent gap, this section will cover the skills gap. We see these two mentioned interchangeably but one is related to quantity (we cannot hire professionals) and the other one to quality (we cannot find qualified/skilled individuals).

Statistics

- **[95%]** Cyber Security skills shortage did not improve over the past few years[14]
  - **[44%]** Say it has only gotten worse
- **[91%]** Say there is a skills disadvantage compared to adversaries[15]
- **[58%]** Cannot find talent with the right skills[16]
- **[35%]** complained about the inability to learn or use the security technologies[17]

We got into a cybersecurity training paradox as ESG, and ISSA is calling it. Added workload is not only contributing to stress and burnout but also to inability to keep up with all the technology changes. Compared to the people we are trying to defend our organizations against we are spending too little time developing new skills or even worse we can not apply what we have learned.

On the positive side increasingly hiring managers are considering earlier experience and direct skills compared to education and certification but even finding the right technical people comes with yet another challenge: human skills.

More organizations recognize the need for human skills as a critical or clear differentiator between candidates. Based on the latest reports and mentioned by ISACAs report, these are the top skills gap, followed by cloud and governance-related skills.

Regulations and data privacy as factors for the increasing need for cyber professionals and the skills gap. In 2019, 60% of the businesses were unprepared for the GDPR, a year later the research conducted by Computerweekly put the figure at 90%.

This is just one example of a skill gap and according to Enterprise Strategy Group, this continues to widen at an alarming rate from 23% to 51% in just two years and doubled in the past 5 years.

The Concordia and European Cyber Security Organization [ECSO] surveys found several learning platforms on the market and the cybersecurity content: Coursera, edX, , and while there are plenty of introductory content for cybersecurity not sufficiently covered are privacy, social engineering, human and social security, risk management, organizational security, and customer service. We keep teaching people technical skills and then expect them to also have business and leadership skills. This is how we built an entire generation of cyber professionals, we focused primarily on how to copy-paste but never how to use critical-thinking, problem solving and some other that became especially important in the past years. As the security function evolved the

[14] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V
[15] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V
[16] HelpNet Security, https://www.helpnetsecurity.com/2022/04/13/modern-enterprise-security-issues/
[17] Hays, Cyber Security Talent Report Addressing the Skills Gap, 2021

expectation is to drop the hoodie, came out from the basement and talk to the business leaders using a lexicon that sounds like foreign language for most technical people. But this is the only way forward.

Previously considered one of the primary sources of candidates, the universities are losing ground as the degree is no longer as important as in the previous years. This can be tied to the fact that skills taught in universities are no longer as important as 5-10 years ago. The industry changed from computing devices to cloud computing, from coding to software development, and from training individuals to do a task to training individuals to be mentors.

Improving Learning & Development

The second keyword for our strategy will be **GROWTH**. Once we have kept our experts within our organizations, we can start building our talent pipeline by building different programs:

- Mentoring and Coaching
- Upskilling and Reskilling
- Career Development Programs
- Reward and Recognition Programs
- Training and Certifications

Organizations must invest in their people to be able to defend its data and people. According to the Hays report from 2021, insufficient funding is the Number ONE cybersecurity challenge. We do not have the human resources to help protect the organizations, but we also lack the investments to remediate the problem.

This is where retention and mentoring/coaching comes into play. The existing professionals already have the technical knowledge to train new people and get them ready for the job. They can also share their business experience and onboard people faster. Reskilling and internal promotions will allow organizations to move people between distinct functions and to start building a talent pipeline. Not only that it will relieve some of the pressure from security and recruitment, but we will bring fresh new perspectives into old problems. It is easier to build technical acumen with someone that already understands the organization's culture, values, mission, and vision.

If we look at (ISC)2 Cybersecurity Workforce Study from 2021 we see that the most important qualifications for cybersecurity professionals are as follows:

- **[38%]** Strong problem solving skills
- **[32%]** Curiosity and eagerness to learn

- **[32%]** Strong communication skills
- **[32%]** Cybersecurity certifications
- **[31%]** Cybersecurity experience

Today's cybersecurity roles are multi-dimensional and are a mix of technical and human skills with a blend of knowledge and abilities to complete a task.

***"The shortage is really dominated by a lack of understanding and adaption on our way of training people and fostering their development in the industry based on the way cybersecurity is evolving"*** Tommaso De Zan

It will take some time until the academia will catch up and change the curricula, so it is up to all of us how much we invest in our people and in our business's future. There is progress but by the time we think everything is settled we will realize that technology and cybersecurity has evolved too much, and we will start all over.

Through the business lens:

- Evaluate and adjust product marketing
- Build a solid management strategy for a strong ROI
- Create demand through awareness and understanding of perceived value

Question to ask ourselves: Are we making strategic or tactical investments?

## Family Affairs

So far, we have investigated the talent and skills gap, and we understand that retention and growth are the way forward to address a part of the problem. Next, we will cover the 'Internal Processes' and understand the relationship between security and business and how this contributed to the overall problem.

Statistics

- **[95%]** Believe there is a gap between current and desired cyber culture[18]
- **[63%]** Complain about security not being included at the start of the projects[19]
- **[54%]** Say their organization will not hire a CISO in the next 12 months[20]
- **[43%]** Replied that business commitment is the biggest factors to decide the level of job satisfaction[21]
- **[41%]** Believe that to improve the relationship between security and business management is important that cybersecurity has a seat at the table in business planning and strategy[22]

As documented by studies conducted by MIT Sloan School of Management and Carnegie Mellon University, effective high-performing teams are characterized by open communication, trust, collaboration, and shared responsibilities among their members[23].

"Enlisting the entire workforce to mitigate the enterprise's cyber risks is an emerging practice", says Doug Grindstaff II, SVP of Cybersecurity Solutions at CMMI Institute.

What are the attributes of an effective cybersecurity culture?

- Employees understand and recognize their role in protecting the organization
- They regularly attend training and workshops
- They do the right thing and report any suspicious activity

The advantages of having a cybersecurity culture are universal and easy to explain:

- Employees will add another layer of defense, the first responders
- Reduced cyber incidents
- Increased visibility and accountability

Another great advantage of a cyberculture-developed organization is less pressure on the cybersecurity teams. By making security everyone's responsibility and employees acting as first

[18] ISACA, The ISACA/CMMI Institute Cybersecurity Culture Report, https://www.isaca.org/-/media/files/isacadp/project/isaca/knowledge-and-insights/info-files/cybersecurity-culture-report.pdf
[19] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V
[20] Hays, Cyber Security Talent Report Addressing the Skills Gap, 2021
[21] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V
[22] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V
[23] ISACA, The ISACA/CMMI Institute Cybersecurity Culture Report, https://www.isaca.org/-/media/files/isacadp/project/isaca/knowledge-and-insights/info-files/cybersecurity-culture-report.pdf

respondents', organizations can protect the existing cyber talent but also create a pool of potential talent.

On one hand we have the business side that is looking at security as a cost center and on the other we have the CISO/security teams complaining about visibility and participation to the organization's strategy and planning.

To compensate for the lack of planning and strategy some companies invest in technologies, which, have never been fully considered from a cyber risk perspective due to the need to quickly implement them in today's hypercompetitive, fast-paced market[24].

We still must make investments in technology to keep the business running but in the same way we need to invest in our people to make sure that technology is also operational and not just another shelf investment.

Improving Internal Processes

The third keyword is **ALIGNEMENT**. A good starting point to improve the cybersecurity culture in an organization and align security with the business is building a Security Awareness Program. This will improve the collaboration between distinct functions, get the necessary visibility in the organization and attract the necessary investment to drive the program and highlight value.

Most cybersecurity people are highly technical individuals, the best at what they do but as already mentioned, this whole field is continuously changing, and we must adapt. While in the past the CISOs responsibility was to create the biggest fence possible, today they need to constantly translate business into security and vice versa.

It is not just about findings and exploiting vulnerabilities but translating that information into risk for the business, how much money to implement and how much money we will lose if we do not. We are no longer the gatekeepers but modern advisors.

I always recommend that people work with other departments and to learn from their best practices (learn from marketing how to sell what you are doing daily, just to share one example). We have so much to learn from each other.

***"Culture eats strategy for breakfast"*** Peter Drucker

[24] Deloitte, The cybersecurity talent shortage An emerging challenge for consumer products companies, https://www2.deloitte.com/us/en/pages/consumer-business/articles/cybersecurity-talent-shortage-consumer-products.html

Through the business lens:

- Aligning strategy, planning and implementation
- Involve customers to share feedback to understand the market

**Question to ask ourselves: Do we understand risk or just ignore it?**

## Financial Outcome

On the last section we are going to cover the financial outcome of not having enough professionals to protect our business, not enough well trained individuals to fill open positions and what happens when communications and collaboration is not practiced enough or effectively inside our organizations. It has become the norm not the exception to see the results of bad security practices and the lack of basic cybersecurity hygiene all over the news and social media.

Statistics

- **[95%]** of data breaches are due to human-error
- **$4.24M** is the average total cost of data breaches [IBM]
- Since 2016 through Business Email Compromise, we have lost **$43 BILLION** [FBI]
- We lose around **$100,000** for every hour of outage and 33% of organizations lose between $1M to $5M
- **50% TO 200%** overall company losses to replace talent (enrich.com)

***"Cybercrime is the number one problem with mankind and cyberattacks a bigger threat to humanity than nuclear weapons"*** Warren Buffet

Cybercriminals are taking advantage of our hyperconnected systems and devices, technology-induced vulnerabilities, human errors, and unprepared organizations[25].

It takes only one successful ransomware attack to destroy a successful business and while most only look at the monetary loss only a few understand that also means that hundreds of employees will be out of work. The same attack can leave hospitals unable to treat people (see the ransomware attack on Ireland's hospitals). You must wonder how many of stories are left untold? How many phishing frauds robbed people's life savings? How many critical systems and infrastructures are under-protected?

What we have seen in the past years is an unprecedented growth of zero-days that made it to the headlines. Many businesses now focus on external-facing systems, fixing critical vulnerabilities, and buying as much time as possible to not end up as another victim. Patching is still a major challenge due to the technical complexity, lack of asset management, and resources.

Securing your organization, already a challenging task is no longer enough as we have seen with the most recent Log4J headlines. Organizations now must consider the security of their suppliers as well, with a high proportion of threats now occurring indirectly from supply chains[26].

The human factor error can be defined as any action that is purposeful or not that creates an information security problem. Not taking into consideration the behavior analytics and not investing in Security Awareness Programs, employees' actions and decision making will go unchanged. It is in human nature to try to circumvent the rules and not follow existing policies as the employees are not helped to understand their role in the bigger picture and how they can help keep the organization secure.

Understanding the human mind is a complex problem that cannot be solved by cybersecurity alone. Research and involvement of cognitive scientists/academia can help organizations shift the technology-only mentality into developing a security culture and awareness and, why not, it could be the more cost-efficient solution overall.

Like any other breakthrough in our history, everything shifts when we start involving experts from other fields and working together as a multi-domain organism with a common purpose – start hacking human behavior as a solution to stop cyber-attacks.

Ajzen's Theory of Planned Behavior [TPB] is simply saying that if the correct behavior is taught, recognized, and rewarded employees will be positive about promoting and engaging in those

[25] Holistica Journal of Business and Public Administration, Botching Human Factors in Cybersecurity in Business Organizations, 19 Dec 2018, https://sciendo.com/article/10.2478/hjbpa-2018-0024
[26] BulletProof, Bulletproof Annual Cyber Security Industry Report 2022, https://www.bulletproof.co.uk/industry-reports/bulletproof-annual-cyber-security-report-2022

activities. Someone that is not helped to understand its role and place, or there is no reward and recognition system in place will be more prone to not carrying what happens after it clicks the link.

Resistance to change is always the change management's biggest challenge but creating a sense of ownership, "Security is everyone's responsibility", along with the motivation for a positive behavior towards doing the right thing can help organization combat the technological determinism while improving security posture and create a security culture where everyone is involved and part of the success.

The human-center cybersecurity concept is for now put on hold. While there are voices in the industry that suggest that this is the right next step, the talent and skill shortage, stress, and burnout paired with the increased complexity of information security requirements make this another item for the wish list.

"*Cybersecurity needs people with diverse backgrounds – business, law enforcement, military, science, liberal arts, marketing design", "Cybersecurity needs you"* says Vasu Jakkal, Corporate Vice President, Security, Compliance, and identity at Microsoft.

Question to ask ourselves: Have we lost enough to start the change?

# TOMORROW

To get to the point of us seeing a dim light and the end of the tunnel we all must work together and be part of the solution. Government, academia, training providers and employers must collaborate, build a lexicon, agree on the skills and knowledge needed in the industry. National policies, academic curricula, and specialized training it is only the beginning to close the gap, there will be always the problem of not having enough people graduating from cybersecurity compared with what the market needs, and these employers must provide internships and apprenticeships, build internal mentoring programs to fill the roles with candidates that are ready to help.

**This is not a time to patch the gap but to find long-term sustainable solutions.**

Next, I will be sharing resources to help organizations start planning and implementing solutions to close the gap. The frameworks and strategies that can build a solid foundation and see existing national strategies, success stories and sources of inspiration.

## Framework

NIST NICE [National Initiative for Cybersecurity Education, USA]

*"The mission of NICE is to energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development" [27]. ("About | NIST")*

This framework is supplying a common language and a set of values and practices to find, recruit, develop, and keep cybersecurity talent. It is supplying resources, tools and guidance for workforce development, planning, training, and education.

[27] NIST, https://www.nist.gov/itl/applied-cybersecurity/nice

The Workforce Framework for Cybersecurity [NICE Framework] ecosystem is enforced by the NIST Special Publication 800-181[28].

What this framework offers are alignment between institutions, academia, organizations, and jobseekers. On the other side is promoting collaboration between institutions, academia, and students to prepare the next generation of cybersecurity professionals by supplying a common structure of up-to-date skills based on the industry needs, see Figure 1 below.


**Figure 1 – Building Blocks for a Capable and Ready Cybersecurity Workforce[29]**

ENISA ECSF [European Cybersecurity Skills Framework, Europe]

*"The mission of the European Union Agency for Cybersecurity [ENISA] is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community"[30].*

Like NICE Framework, ECSF is also proposing a similar framework with the goal of connecting industries, academia, and the workforce and develop a common language towards skills, roles, and knowledge.

[28] NIST, https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final
[29] NIST, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf
[30] ENISA, https://www.enisa.europa.eu/

SFIA [Skills Framework for the Information Age][31]

The Skills Framework for the Information Age is the global skills and competency framework for the digital world. ("The global skills and competency framework for a digital world") It is a model for describing and managing skills and competencies for professionals working in information and communications technology, software engineering, and digital transformation[32].

## Strategy

NCSC [National Cyber Security Centre, United Kingdom][33]

This initiative was the result of UKs Cyber Security Strategy, and its goals are to:

- Attract more students to study cybersecurity
- Connect employers and employees supplying a common lexicon of skills and knowledge

ACCSEs [Academic Centers of Cybersecurity Excellence, Australia][34]

As part of the Australian Cyber Security Center and cybersecurity strategy, two academic centers were set up to help with the country's strategic vision and in collaboration with the Minister of Education and Training. Goals:

- Collaboration between universities, employers, and the government
- Building effective strategies and programs to develop cybersecurity talent
- Involve the private sector

ANSSI [The National Cybersecurity Agency of France][35]

One of ANSSIs responsibilities is to connect students and employers offering a lexicon for both parties. Like all other mentioned efforts, it is another example of how governments, academia, professional associations, and the industry can work together towards a common goal.

[31] SFIA, https://sfia-online.org/en
[32] Wikipedia, https://en.wikipedia.org/wiki/Skills_Framework_for_the_Information_Age
[33] NCSC, https://www.ncsc.gov.uk/
[34] ACCSE, https://www.cyber.gov.au/acsc/view-all-content/glossary/academic-centres-cyber-security-excellence-accse
[35] ANSSI, https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/

The countries, hubs and initiatives mentioned above might have different strategies but similar goals, to connect everyone from the highest levels to students, to supply a common language and to overall, close the talent gap.

It is not going to happen overnight, but the path is there, and more are following it. We must work together and build one standard framework that can be followed and adjusted based on every country capability and industry expectations.

Some other efforts worth mentioning are related to Australia, Estonia, Japan, Netherlands, Singapore, UK, and US strategies around educational activities targeting preschool and general education. These include training teachers and personnel, making computer science and digital skills mandatory.

Next, we will mention about some of the efforts that governments have done (or plan to do) to reduce the talent and skills shortage:

1. Primary & secondary school
    - Revision of the curricula (to add security and technology)
    - Adding more cybersecurity competitions
    - Training for teachers and personnel
2. Higher Education & research
    - Cybersecurity competitions
    - Scholarships and grants
    - Creating more academic centers of excellence
    - New degrees and programs
    - Integration of cybersecurity awareness into all higher education programs
    - Collaboration between industry and academia
    - Investments in cybersecurity research
3. Workforce
    - Cybersecurity qualification and competency frameworks
    - Workforce reskilling programs

## Implementation

Bringing new candidates into the cybersecurity field, increasing the talent pool by focusing on under-represented groups will help build a human capital pipeline.

According to ISACA's State of Cybersecurity Report 2022

One way to mitigate the technical skills gap is to train non-security staff and move them into security roles or to use consultants. The first one can become a solution with the proper investments and correct programs as for using consultants, which is just for the short term until your next cyber generation is ready to take on defending the organization.

According to Hays Cyber Security Talent Report

Organizations must become visible and say what they are doing and to say they want to do in the future. There is the idea that only cybersecurity teams do security, but that is outdated, today everyone is doing or trying to do security. Participate at career fairs, and local events and share your desire to hire cyber talent.

Look inside for people that want to re-skill and try cybersecurity. Offer enough opportunities to train and mentor and look beyond the technical skills needed for the job. According to the trends, entry-level jobs are considering more things like attention to details, analytical thinking and problem solving, and one of my favorites, customer skills.

To start building your talent pipeline and attract new talent we need to revisit our requirements and prioritize what is important to grow our team and our business. As more professionals say, job descriptions are today just a laundry list of wishes and desires.

Partner with your local institutions and start building bridges, offer opportunities so any cyber aspirant can experience learning firsthand skills and get prepared for their first job in the field.

Organize workshops and start being visible in the community.

Everyone wants an opportunity to gain experience and work with skilled professionals that have competitive salaries and benefits and an environment that supports development and recognition.

1. Understanding and evaluate your current environment and salaries
2. Re-evaluate job requirements. Current job descriptions might discourage some potential candidates; try to use a system and assign responsibilities from entry-level to senior management

3. Language bias.
4. Candidate centric hiring process

### *Diversity, Equity, and Inclusion [DEI]*

McKinsey shows that companies in the top quartile for gender diversity are 25% more likely to have industry-leading profitability compared to companies in the bottom quartile. For ethnic diversity, that number increases to 36%, and for disability, it's 28%[36].

Broadening the search for talent, offering opportunities to gain experience, new skills, apprenticeships, internships and other programs seems one way to approach this problem. Recruiting based on a four-year degree will automatically exclude "84% of Latinos and 78% of the African American from the get-go" says Gerald Chertavian, founder and CEO of Year Up.

Diversity can play a significant role in helping organizations close the talent gap. ("Upskilling, better training keys to increasing cyber ...") Promoting advancements of minorities through mentoring programs, offering equal promotion opportunities while being intentional and deliberate about keeping employees will get the best out of everyone.

According to Cybersecurity Ventures *"women represented 25 percent of the global cybersecurity workforce in 2021, up from 20 percent in 2019, and 10 percent in 2011".*

DELL'S PROJECT IMMERSION[37]

In January 2019, Dell started a partnership US Historically Black Colleges and Universities [HBCUs], minority-serving institutions [MSIs] and Hispanic serving institutions [HSIs] to equip students with the knowledge and skills they need to succeed in the technology industry.

[36] McKinsey, https://www.mckinsey.com/featured-insights/diversity-and-inclusion/diversity-wins-how-inclusion-matters

[37] DELL, https://www.dell.com/en-us/dt/corporate/social-impact/cultivating-inclusion/workforce-of-the-future.htm

"Dell Technologies believes closing the diversity gap is critical to meeting future talent needs and ensuring that new perspectives reflect our global customer base"

Dell Technologies 2021 Diversity and Inclusion Report. ("investors.delltechnologies.com")

Apple, Facebook [Meta], Microsoft and Google also have announced their diversity and inclusion programs but have made little progress compared to Dell's program. The difference stands with Dell's strategic partnering with colleges and universities around US, prioritizing content around emerging and disruptive technologies and following concept to execution.

Another success factor was making the program visible to attract students, sponsoring job preparation events, and adjusting to the current needs.

The results:

- Dell increased its hiring with Project Immersion talent pools by 37%
- Increased acceptance and response from the community

"Project Immersion has taken a small step towards international expansion by starting a cybersecurity pilot at a college in Brazil".

In 2020, the same company started a hiring program for people with autism, several Employee Resource Groups, and various initiatives for reskilling today's talent for the future[38].

IBM'S NEW COLLAR PROGRAM[39]

*"IBM's New Collar initiative focuses on improving access to opportunities for people who come from non-traditional backgrounds. In today's modern world, IBM understands that hiring good talent does not just mean hiring someone with a diploma. It is about having the right skills, practical experience, and the determination to succeed."*

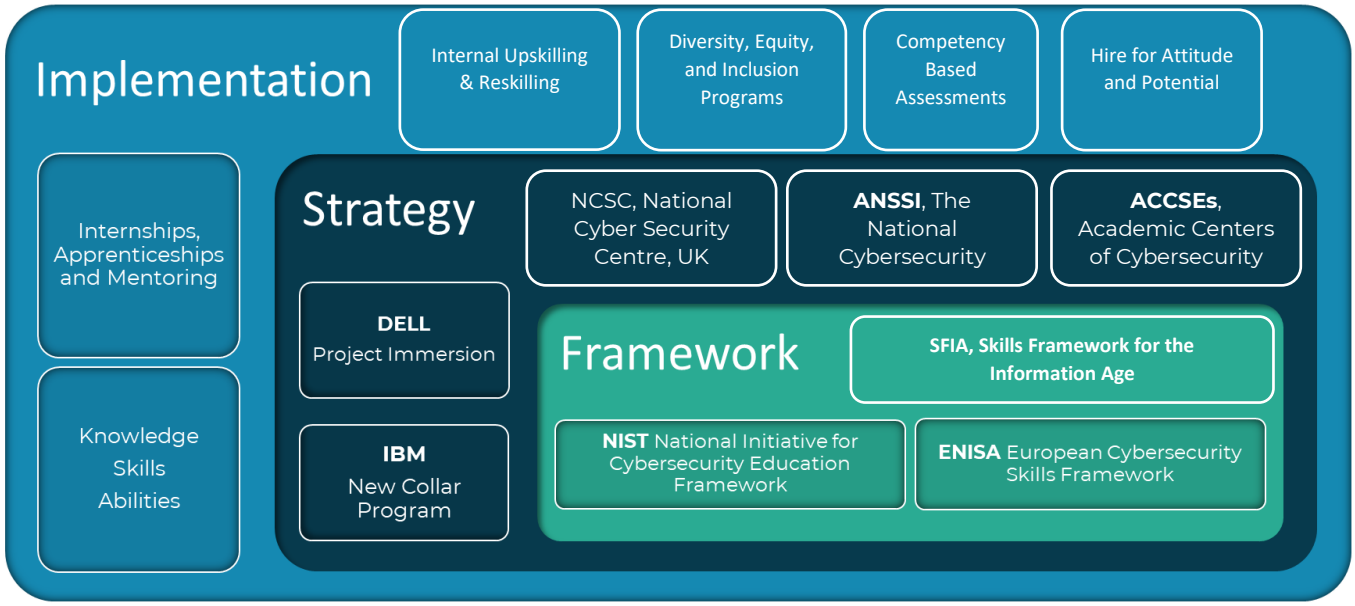
According to the World Economic Forum (WEF), closing the global skills gap could add US$11.5 trillion to global GDP by 2028. To help do so, according to the WEF, the public and private sectors need to collaborate on education and training that keeps pace with market demands,

[38] Dell, https://www.dell.com/en-us/blog/the-talent-gap-building-a-bridge-to-the-other-side/
[39] IBM, https://www.ibm.com/us-en/employment/newcollar/index.html

demographic changes, and technology progress. ("IBM Commits to Skill 30 Million People Globally by 2030 - Insider")

IBM's commitment is to provide 30 million people with the skills needed by 2030. To achieve this goal, IBM is announcing a clear roadmap with more than 170 new academic and industry partnerships[40]. ("IBM Commits to Skill 30 million People Globally by 2030"). ("IBM Commits to Skill 30 Million People Globally by 2030")

Simple representation of how proposed frameworks, strategy and implementation can work together to close the talent and skills gap.




There is no simple solution to this problem, or shortcuts, or tactical investments only long term planning and commitment. It will take all of us to grow the next generation of cyber professionals and build a better and more secure tomorrow.

[40] IBM, https://newsroom.ibm.com/2021-10-13-IBM-Commits-to-Skill-30-Million-People-Globally-by-2030