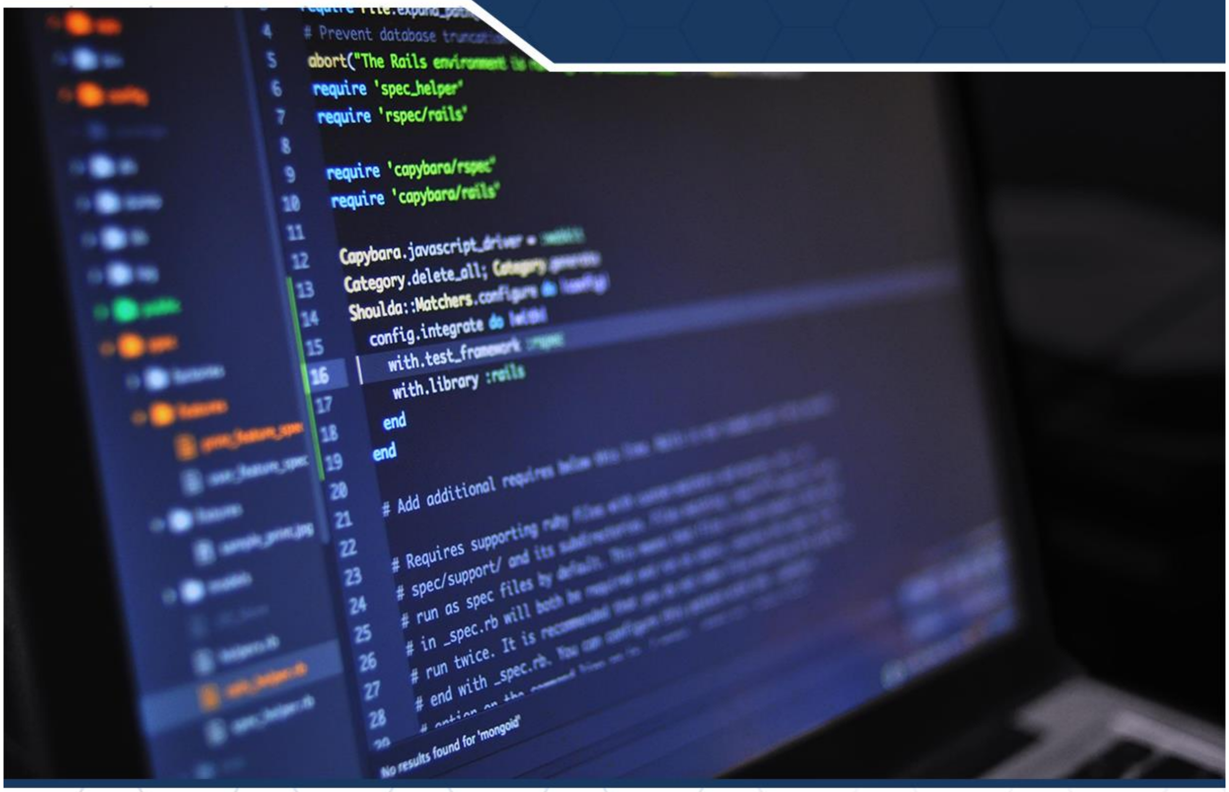
Skills Shortages in Cyber Security



```
# Prevent database truncat
abort("The Rails environment
require 'spec_helper'
require 'rspec/rails'

require 'capybara/rspec'
require 'capybara/rails'

Capybara.javascript_driver =
Category.delete_all; Category
Shoulda::Matchers.configure do |config|
  config.integrate do |with|
    with.test_framework :rspec
    with.library :rails
  end
end

# Add additional requires below

# Requires supporting ruby files
# spec/support/ and its subdirectories
# run as spec files by default
# in _spec.rb will both be required
# run twice. It is recommended
# end with _spec.rb. You can configure
No results found for 'mongoid'
```

A bluedog Whitepaper

bluedog SECURITY MONITORING

Skills Shortages in Cyber Security

And How they Affect Your Business

Executive Summary

Every day we hear about a new company that was hacked. The cyber-threats grow more diverse and more numerous by the minute. Even more worrisome is the fact that we don't hear about most companies being hacked – just the ones big enough to impact the data of thousands or millions of their users or customers.

Perhaps your company didn't face a cyber-threat yet. But this doesn't mean it won't.

As the number of attacks on companies of all sizes grows, the number of cybersecurity professionals doesn't. The gap between supply and demand is huge in this industry and growing at an accelerated pace.

More importantly, even people who are security professionals have to constantly update their skills and learn how to defend against the newest threats. In a sense, it's not just a human resources shortage we're dealing with, but also a literal skill shortage – people who work in this industry aren't always prepared to mitigate any threat. They are hyper-specialized, which means that one company needs to hire an entire team, not just one security expert.

Just how bad is the cyber security skills shortage worldwide?

How can business owners protect their assets under these circumstances?

Who is most affected by the skills shortage?

How can you mitigate threats with a skeleton team to no security team in place?

This whitepaper will answer all the questions above and offer an inside perspective on how SMEs can cope with a situation that most likely won't be sorted out anytime soon.

Table of Contents

Executive Summary 2

Skills Shortages in Cyber Security – An Overview 4

A Growing Number of Diverse Threats to Enterprise Security 9

The Solution: A Pro-Active and Granular Approach to Enterprise Security 12

A Pro-Active Approach to Security Concerns 12

A Granular Approach to Security Concerns 13

About BlueDog Security Monitoring 14

Skills Shortages in Cyber Security – An Overview

A recent study[1] conducted in the UK by the Department for Digital, Culture, Media & Sport (DCMS) found that a worrying number of companies cannot find the skilled professionals they need for cyber security tasks. We're not even talking about complex skill sets here.

48% of the UK companies (or 653,000) cannot carry basic tasks defined in the Cyber Essentials[2] scheme issued by the government. Things like setting up firewalls, removing malware or storing data in a secure manner are too complicated for almost half the businesses in the UK.

Another 30% of the surveyed UK companies (or 408,000) lack advanced cyber security skills like pen testing, security architecture or forensics.

The same report found that 64% of the organizations admitted to having problems because of the cyber security skills gap, while 25% of them said that this has negatively impacted their business. Furthermore, 35% of firms say that it's hard to recruit in this industry. Their cyber security vacancies are hard to fill because the applicants lack the technical skills and knowledge required for the job.

3 out of 10 companies also reported that applicants lack non-technical skills like communication or leadership, which prevents them from meeting their business goals.

68% of companies in the cyber sector tried to recruit someone in a cyber-security role within the last 3 years, but 35% of these vacancies have been reported as "hard to fill". Generalist cyber roles have also been deemed hard to fill in 51% of cases. Out of these, the hardest ones to fill are for senior staff (3 to 5 years of experience) and principal level staff (6 to 9 years of experience).

The most in-demand roles are:

- Security engineers
- Security analysts
- Security architects
- Security managers

[1] https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020, retrieved September 2020

[2] https://www.ncsc.gov.uk/cyberessentials/overview, retrieved September 2020

- Security consultants

The sectors where cyber specialists are most in demand are finance and insurance, communications, information and professional services.

The areas with the biggest shortage of technical skills in the UK, according to the same report, are:

- Information risk management
- Testing or compliance
- Management and governance
- Research in cyber security
- Secure systems implementation

The situation is equally dire all over the world, not just in the UK. A McAffee report[3] analysed the cyber security skills shortage in eight countries, with equally worrisome results.

[3] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf, retrieved September 2020

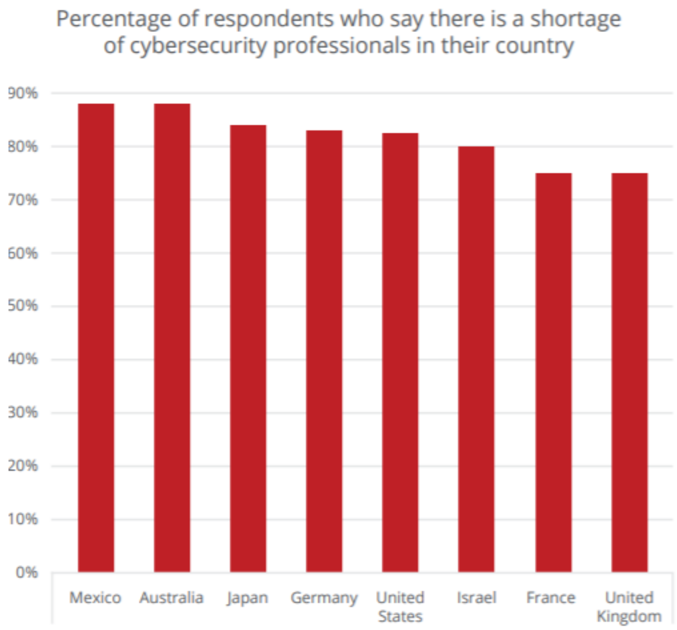
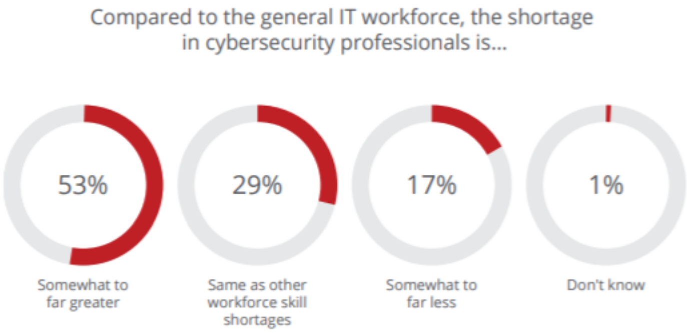


Figure 1. Cybersecurity workforce shortages by country and skillset.



82% of the respondents in Australia, France, Germany Israel, Japan, Mexico, the UK, and the US agree that there is a skills shortage in their organisation, as well as in their entire country. In 2019, two million jobs in cyber security were left unfilled globally.

The cyber security shortage also has second-order effects. For instance, the average salary in the industry is much higher than the median salary in that country (at least 2.7 times higher).

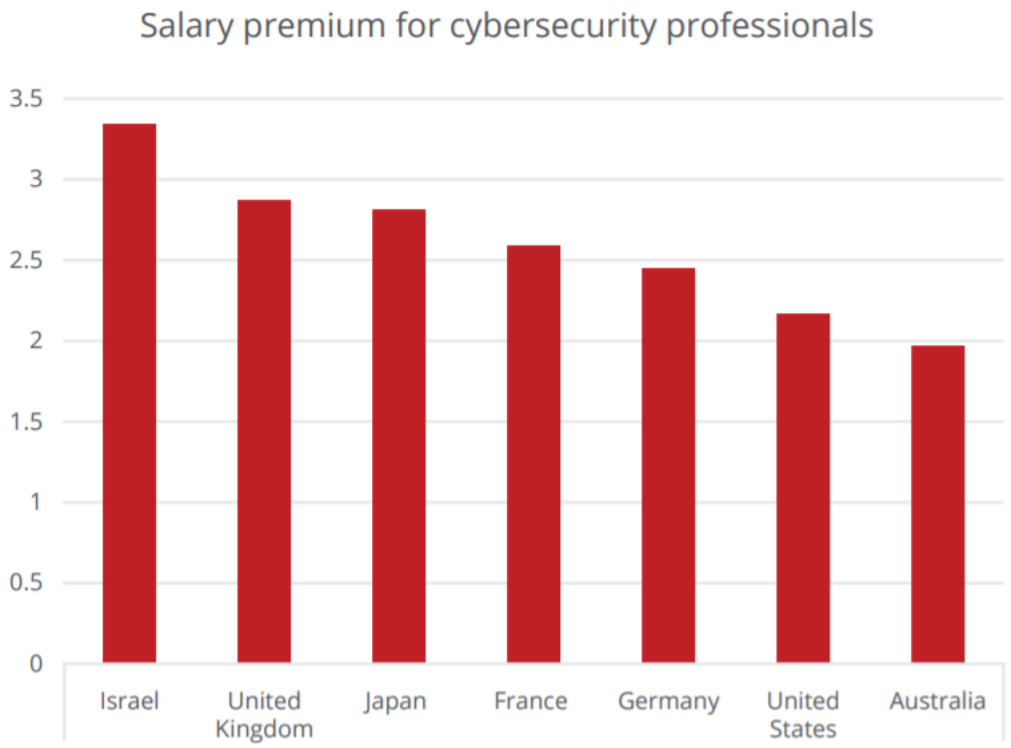


Figure 3. Cybersecurity salary premium (annual average salary from survey compared to OECD average annual wages).[8]

This workforce gap has already caused companies all over the world to incur significant damage.

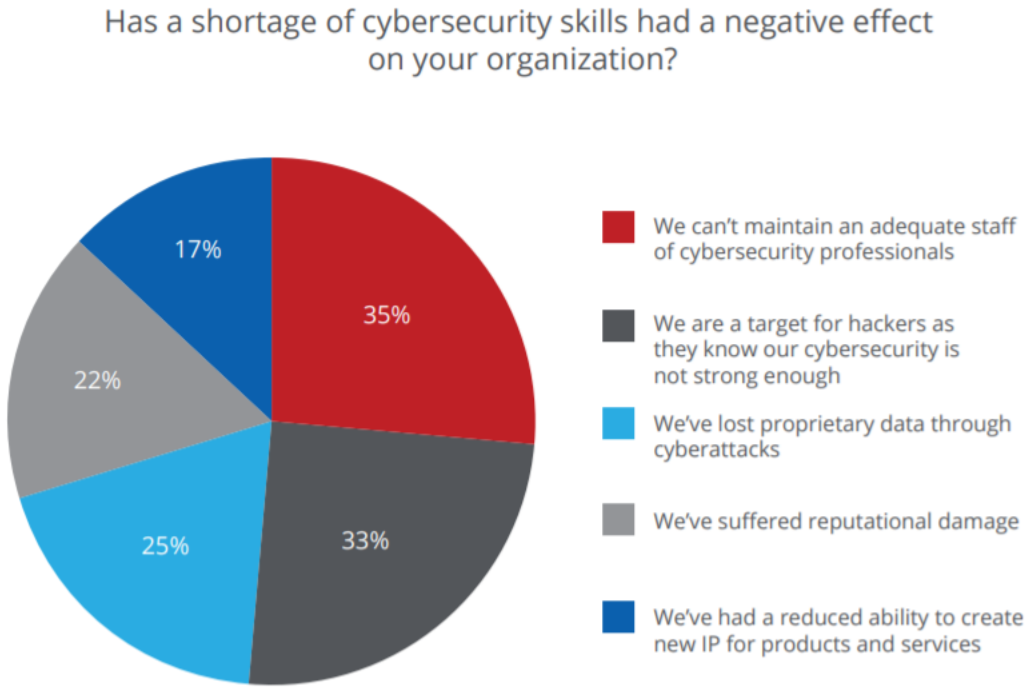


Figure 5. Impact of cybersecurity workforce shortage.

If the salaries in cyber security are well above average and it wouldn't be hard to find a job anywhere in the world, why the shortage of skilled professionals?

The answer seems to be in the process of acquiring the skills. While higher education is important and a bachelor's degree is the minimum entry barrier in this field, university classes alone cannot prepare the cyber security specialists the industry needs.

The threats evolve quickly and they evolve constantly. Which means education has to be equally constant and that cyber security skills grow obsolete very fast.

Non-traditional sources of education and self-starters are always preferred in this field. Especially since the bulk of their education in cyber security will happen long after graduation, in a fast-paced, hands-on manner.

The next chapter will shed some light on why constant education is the most important building block in a cyber-security specialist's skill set.

A Growing Number of Diverse Threats to Enterprise Security

This is the Catch-22 of the cyber security industry: there are fewer and fewer skilled specialists and more and more cyber-attacks. In a way, it makes perfect sense: with less “guardians” to guard business assets, cyber criminals have an easier job at planning their attacks.

The COVID-19 pandemic sent people from offices to work from home. 51% of cyber security professionals said that their organisation is at moderate or extreme risks for attacks[4]. And that was before the pandemic, when every computer or device connected to the company network underwent at least *some* security screening.

Now, the situation is even direr. Employees work from unsecure home networks and a return to a completely “normal” office life is not yet possible[5].

We now see more than 4000 attacks per day, every day[6], a 400% increase from the before-coronavirus era. Large corporations, government institutions and critical infrastructure are the major targets. However, SMEs and individuals haven’t been spared either, even though most of the official statistics available to the public focus on the attacks that make the most damage.

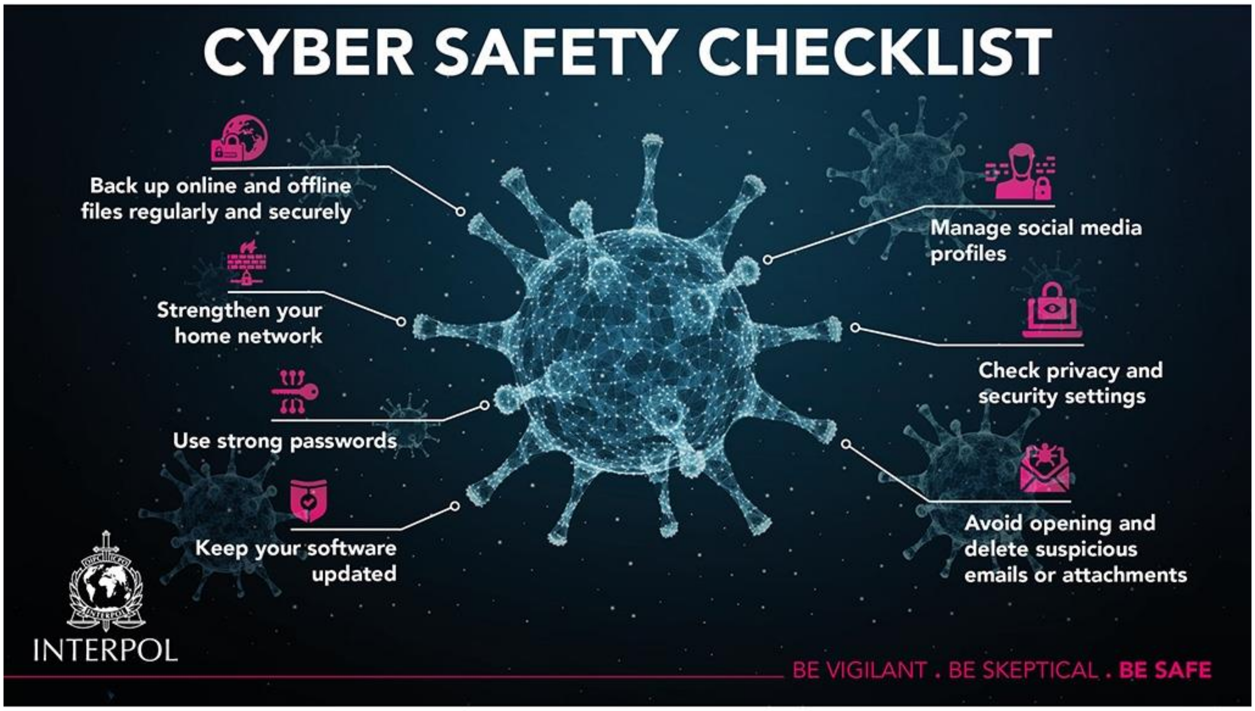
The Interpol makes generic recommendations[7] about cyber security at home and in the office – or in-between, as most of us spend our working days now.

[4] https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-tops/, retrieved September 2020

[5] https://www.weforum.org/agenda/2020/08/office-work-coronavirus-covid-19-saftey-employment/, retrieved September 2020

[6] https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html, retrieved September 2020

[7] https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats, retrieved September 2020


CYBER SAFETY CHECKLIST
Back up online and offline files regularly and securely
Strengthen your home network
Use strong passwords
Keep your software updated
Manage social media profiles
Check privacy and security settings
Avoid opening and delete suspicious emails or attachments
INTERPOL
BE VIGILANT . BE SKEPTICAL . BE SAFE

Malicious domains, malware and ransomware are the top types of attacks used by cyber criminals right now. For each large corporations, there are at least a few dozens of SMEs who suffer breaches every day.

We see it in our own statistics at Bluedog Security. More and more SMEs are interested in our Managed Detection and Response service[8], as well as in our Microsoft Office 365 Security Monitoring service[9], both of which are clear signs of an increased number of attacks, on one hand and of an increasing remote workforce that needs security, on the other hand.

But more on that later.

For now, our conclusion, as well as that of cyber security professionals everywhere, is simple but alarming: companies of all sizes, and especially SMEs are more at risk than ever. The growing skills shortage in the industry, coupled with the increased number of attacks makes usual solutions out of reach. Who can afford to hire a top team of cyber security professionals?

[8] https://bluedog-security.com/managed-detection-and-response/, retrieved September 2020
[9] https://bluedog-security.com/microsoftoffice365securitymonitoring/, retrieved September 2020

Very few companies! This is why the solution needs to match the issue: it has to be out-of-the-box and tailor-made to the current threats.

Let’s take a look at it!

The Solution: A Pro-Active and Granular Approach to Enterprise Security

As mentioned before, there is little hope for the average SME to hire a full cyber security team. The initial chapter of this whitepaper also revealed that finding a single specialist to mitigate all the threats in the fast-paced cyber-attacks landscape is impossible.

So what can SME owners do? Wreak havoc on their budget and harm their growth to ensure that their security is on point?

There's no need for dramatic measures.

We suggest a two-pronged approach.

A Pro-Active Approach to Security Concerns

First and foremost, you should not wait for the first attack to happen. By then, you will have lost more money (directly or indirectly through data leaks and bad press) than if you would have taken the pro-active approach.

Regular vulnerability scans[10] and pen tests[11] are a must, irrespective of the size of your company. We recommend them for solopreneurs and for companies with more than 1000 employees. If you have a computer or a device that is connected to the internet, you need these services.

As their names suggests, their main advantage is the fact that they can tell you which of your assets are vulnerable. A skilled pen tester can reveal the types of attacks your network or devices are vulnerable to and, of course, come up with ways to enhance your security.

More importantly, regular pen tests and vulnerability scans can also detect if a breach *did* happen. It's not ideal to identify after the attacker has managed to penetrate your network, but it's still better than not being able to advise your customers or stakeholders that their data has been breached on your own time.

Worried that it's *still* hard to find specialists for these tests and scans?

This is why we have the second tier of our approach.

[10] https://bluedog-security.com/vulnerability-scanning/, retrieved September 2020
[11] https://bluedog-security.com/penetration-testing/, retrieved September 2020

A Granular Approach to Security Concerns

You don’t have to pay hundreds of thousands of dollars every year for a security specialist who knows *everything.* What you can do instead is hire a security partner that comes with their own team.

In most cases, a complete security team is over the top – you don’t need four or five specialists to work full time for an indefinite amount of time if you run a SME. This is what companies like Bluedog Security Monitoring are for.

They offer you the complete expertise of an entire cyber security team at a fraction of the cost. A company like Bluedog Security Monitoring can help you mitigate both cyber threats and budget chaos.

A granular approach to security doesn’t mean that you will only get part of the full picture. Quite the opposite. It means that you can outsource parts of your security concerns to one or more providers.

For instance, if you know that your company is more exposed to risks since your staff is working remotely, our Microsoft Office 365 Security service is ideal for you. Want to go the extra mile? Why not make sure all your software and your devices are safe with vulnerability scanning and pen testing?

This type of granular approach gives you more than peace of mind. It also gives you a complete overview of your security strong and weak suits at a fraction of the cost of hiring an in-house specialist.

About BlueDog Security Monitoring

Our goal is to provide businesses with a level of network protection typically only afforded by large corporations. We aim to bring high-quality technology, support, and service to the small to medium business, helping protect their business from cyber threats.

Our company is growing quickly, through our simple and affordable end-to-end network monitoring solution. Recently voted one of the Top 10 cybersecurity start-ups of 2019 by Enterprise Security Magazine. Whether you are a small business, or an MSP or IT services reseller or distributor, get in touch and have a chat with us.

20-22 Wenlock Road, London, N1 7GU

info@bluedogsec.com

+44 20 8819 6254