Franklin Fitch

Safeguarding SMBs: An Insight into Network Security Threats

www.franklinfitch.com

CONTENTS

WHAT ARE THE COSTS OF CYBER ATTACKS TO US SMBS?

In their Cost of a Data Breach Report 2024, IBM reported that the average cost of a data breach caused by a cyber and network security attack increased by 10% compared to the previous year. As a result, the average cost of a data breach in 2024 reached record highs of $4.88 million.

Moreover, according to Security Magazine, over 800,000 attacks happen each year, equating to more than 2,200 attacks per day and one attack every 39 seconds. Statista has also estimated that the costs of cybercrime could climb from over $9 trillion recorded in 2024 to more than $13 trillion by 2028.

These alarming statistics clearly highlight how significant cyber and network security attacks can be and how they're continuing to become more of a problem with no signs of slowing down. With the clear potential to cause severe financial damages, these threats can also cause reputational harm, resulting in the exploitation of an organization's internal and external private data.

$4.88 million

The average cost of a data breach in 2024

39 seconds

One attack every 39 seconds

$13 trillion

The estimated cost of cybercrime by 2028

BUT BUT HOW DOES THIS IMPACT SMALL AND MEDIUM-SIZED BUSINESSES?

Most modern enterprises utilize some form of IT infrastructure and networks to varying degrees. Whether you rely on networks to power the majority of your business operations or just a small proportion, you run the risk of falling victim to an attack. Regardless of your business and the industry you operate in, every SMB needs network security.

> **“IT infrastructure is industry agnostic. Every business needs a solid foundation of network security.”**
>
> – Martin Rennison, Director of Contracts

Awareness of cyber, and more specifically, network security, is essential in today’s fast-moving tech world, especially for small and medium-sized businesses. While cybersecurity protects the data stored within a network, network security focuses on safeguarding an IT infrastructure, ensuring online communication and data sharing are carried out securely.

With insight from our in-house network security experts, we will explore the key discussions regarding SMBs and network security. You will discover why SMBs are at a higher risk of network security threats and the main types of attacks that could cause severe damage to your business.

From there, we will outline how your SMB can prevent network security attacks before highlighting the importance of prioritizing your network recruitment strategy and benchmarking your network security salaries.

WHY ARE SMBS AT A HIGHER RISK OF NETWORK SECURITY THREATS?

As of 2024, there are over 33 million small businesses in the US alone. According to the ITRC Business Impact Report, 73% of US small businesses were said to have fallen victim to a cyber breach or data attack in 2023. These attacks cost 13% of these businesses over $500,000 in damages. The National Cybersecurity Alliance has also stated that around 60% of small businesses shut down within six months as a result of being hacked.

But why is this, and why is the IT infrastructure of an SMB more likely to be the victim of network security threats?

MISCONCEPTIONS ABOUT BEING TARGETS

A common misconception among many SMBs is that due to their size, they are of no value to cybercriminals. As reported by OpenText's Global SMB Ransomware survey, **67% of SMBs do not consider themselves targets** for ransomware**.** This alarming statistic highlights a worrying lack of awareness among SMBs regarding the risks associated with their businesses and network security threats. In reality, if these misconceptions are not addressed, they could result in severe damage.

73%

Of US small businesses experienced an attack

$500,000+

The cost of an attack by 13% of US small businesses

60%

Of US small businesses close within six months as a result of an attack

SMBS ARE ATTRACTIVE TARGETS FOR HACKERS

Despite their size, hackers actually perceive SMBs as more appealing targets because their network security defenses are often considered weaker. They are also aware that SMBs often have connections with and work on behalf of major global organizations.

As a result, they know SMBs will hold valuable data, such as company bank details, employee records, and email addresses. Hackers will infiltrate an SMB's network as a gateway to exploit this sensitive information.

HUMAN ERROR AND LACK OF TRAINING

According to Verizon's 2023 Data Breach Investigations Report (DBIR), **74% of data breaches were caused by human error.** Employees within an SMB who are unaware of or haven't been provided with relevant training on how to detect a network security threat could unintentionally cause a business to fall victim to an attack.

> **"I think some SMBs see that something's gone wrong and realize they've got a problem when an attack has occurred. Or it could be that they've conducted a security review and thought about what they can do that's best practice to prevent an attack."**
>
> – Martin Rennison, Director of Contracts

LACK OF INVESTMENT IN NETWORK SECURITY

SMBs often prioritize cost-cutting measures as they plan their growth strategies. Due to a lack of awareness and misconceptions about network threats, they often neglect to invest in network security measures. This lack of investment in network security tools, internal awareness training, and recruitment could make an SMB's cost-cutting strategies redundant if they become casualties of an attack.

NETWORK SECURITY ATTACKS SMBS MUST KNOW

SMBs are prone to being vulnerable to network security threats. Carried out by malicious parties who are becoming more sophisticated by the day, prominent and emerging threats can significantly disrupt a business's daily operations. Before learning how you can prevent these attacks from impacting your organization, you must recognize the core types of network security threats.

PHISHING

Phishing is a common social engineering attack in which a cybercriminal uses deceptive tactics to access private information. Typically, phishing attacks take the form of fake emails or messages sent via online platforms. These messages contain links to malicious sites or files. At face value, these messages seem legitimate, but if clicked on or downloaded, they can infiltrate and corrupt a network, allowing the hacker access to exploit sensitive data.

"Phishing-based attacks and social manipulation are often the easiest ways. SMBs often lack internal training and can be targets for phishing emails. If they don't have good filtering, then all it takes is one click for a hacker to infiltrate the network."

– Joe James, IT Support Engineer

DENIAL OF SERVICE

Denial of Service (DoS) attacks focus on sending vast amounts of traffic to overwhelm a network. Cybercriminals will use multiple devices to flood the network with requests, causing it to become overloaded and unable to decipher legitimate users from malicious parties. DoS attacks can cause significant disruptions and downtime to normal operations, which can cost SMBs both financially and reputationally.

"Denial of Service attacks happen when a malicious party sends a lot of bot traffic to completely take down your system. If you're working in something like infrastructure and your service goes down, it can significantly impact your operations."

– Joe James, IT Support Engineer

MALWARE

Malware attacks come in various forms and are harmful pieces of software designed to infect a network and damage, modify, or disrupt a company's IT infrastructure. Common types of malware include **viruses** that replicate to damage sensitive data, **worms** that spread viruses often through emails, **trojans** disguised as legitimate software, and **spyware** that tracks user activities to steal sensitive data.

RANSOMWARE

Ransomware is a prominent type of malware used by hackers to blackmail users. Malicious parties will encrypt or threaten to infiltrate a network unless the user makes a ransom payment. Ransomware as a Service (RaaS) is a widely used service that allows cybercriminals to share variants and launch attacks with ease.

> **"In the US, I see a concern around ransomware attacks. SMB clients of mine that have a lot of critical infrastructure, financially these businesses are a lot less likely to be able to afford the consequences of a ransomware attack."**
>
> – Manuel Osaba, Principal Consultant
> - Network and Network Security

3.4 billion

Phishing emails are sent daily

$6,000 per min

The average cost of a DoS attack in 2023

6 billion

Malware attacks recorded in 2023

$265 billion

Forecasted damages of ransomware attacks by 2031

HOW SMBS CAN PREVENT NETWORK SECURITY ATTACKS

SMBs can take several approaches to prevent network security threats from impacting their business.

Many of these techniques are similar to those of a **cybersecurity** strategy and consist of implementing a disaster recovery strategy, training end-users, deploying firewalls, utilizing multi-factor authentication, applying encryption, and introducing vendor consolidation. Developing and deploying a comprehensive network security strategy is essential for SMBs to safeguard their networks and infrastructure. Doing so can be the difference between a company falling victim to threats that could hinder the future of the business and prospering in the tech-driven world. With insight from our specialist consultants, this section will outline the core ways SMBs can prevent network security attacks.

"Some SMBs are forward-thinking, but many often realize that something has gone wrong when it's too late, and they can't afford to let it happen again. All SMBs need solutions to prevent network attacks from impacting their operations."

– Martin Rennison, Director of Contracts

IMPLEMENT A DISASTER RECOVERY STRATEGY

Disaster recovery strategies involve implementing various procedures and policies to safeguard a network against various threats. Robust recovery plans initially include conducting a thorough security assessment of the business. Here, companies should identify potential vulnerabilities to the network and analyze employee behavior and internal processes regarding network security.

Once vulnerabilities and internal practices have been identified and analyzed, a company should begin planning its approach to preventing network security threats. This plan should factor in safeguarding local, wide, and wireless networks, along with any additional network applications, data, and services the business uses.

> **"It's super important to have a disaster policy so your engineers know exactly what to do when your business is faced with a network security attack. It's not necessarily preventative, but it can help resolve security-related issues pretty quickly. I think it's significantly important for organizations, especially SMBs that may not have these policies, to build them and think about what they can do in the event of an attack."**
>
> – Joe James, IT Support Engineer

The goal of the disaster recovery strategy is to help restore a network in the event of a network security attack. It allows for regular data backups, safeguarding a business against data loss from a network threat or system failure and ensuring sensitive and private information remains secure and accessible to those with authorized access.

TRAIN YOUR END-USERS

Your employees are the first line of defense against network threats. Regardless of their role, whether technical or non-technical, they can detect and even prevent network attacks from impacting your business. Your staff must receive training to ensure they have the know-how to defend the company's infrastructure from potential threats.

> **"SMBs should be educating their users. When it comes to something like phishing, are your users aware of what they should and shouldn't be clicking?"**
>
> – Martin Rennison, Director of Contracts

SMBs should conduct regular cyber and network security training to ensure their employees understand the various threats and the measures they can take to mitigate them. This training could include detecting and avoiding phishing emails, creating strong and regularly updated passwords, and following safe internet practices, such as avoiding public Wi-Fi when accessing company resources. It should also teach them how to report a potential threat or suspicious activity.

Network security training could be conducted with support from an external training provider or by an internal network security expert. Taking these training measures can put your employees at ease when working on your networks and IT infrastructure.

DEPLOY FIREWALLS

Firewalls should be a non-negotiable must-have for SMBs looking to prevent network security attacks. They play a vital part in creating barriers against malicious parties and unauthorized traffic. It's essential for SMBs not only to install but regularly update their firewalls with the latest security configurations and patches.

SMBs should also consider deploying Next-Generation Firewalls (NGFWs). NGFWs are a type of firewall powered by the latest threat intelligence and device filtering, giving networks additional protection over traditional firewalls.

Deploying firewalls into your business is relatively straightforward, especially if you have the proper third-party support and internal personnel to support you. The type of firewall your SMB adopts will depend on the security vendor you partner with. This will also influence the type of network security professional you hire. Later in this insight report, we'll discuss vendors and the importance of acquiring the internal support of network security specialists.

APPLY MULTI-FACTOR AUTHENTICATION (MFA) AND ENCRYPTION

Another way SMBs can prevent network attacks from impacting their business is to introduce MFA and encryption into their operations. Firstly, MFA gives companies an extra layer of security, requiring end users to input multiple credentials before accessing information and data.

Multi-factor authentication can consist of applying unique and complex passwords that are updated frequently to prevent password compromises and data breaches. It can also involve the user completing multiple verification steps before accessing the data. These steps could include inputting several passwords and codes to biometric information such as facial and fingerprint scanners.

Encryption is another vital approach to network security worth implementing and involves converting private data into a code known as ciphertext. Only users with authorized access can unlock this code with the necessary decryption key. The encryption process means that even if a cybercriminal gains access to the encrypted data, they won't gain official access without the decryption key.

Utilizing MFA and applying encryption can significantly enhance your network security posture, making it challenging for hackers to access and infiltrate your private data and sensitive information.

FACTOR IN VENDOR CONSOLIDATION

One final way SMBs can enhance their network security posture and prevent network threats is to factor in vendor consolidation. Cisco, Fortinet, and Palo Alto are the three top vendors we see our clients utilize with great success.

However, rather than investing in various third parties to protect your infrastructure, choosing one vendor that meets all your IT and security-related requirements is the best practice.

“We typically see Fortinet, Palo Alto and Cisco as the top security vendors.”

– Jacob Stevens, Senior Consultant - Network and Network Security

Cisco

Fortinet

Palo Alto

A unified approach to the vendor you select makes managing your network security and IT infrastructure more seamless. Since you'll only invest in one vendor, you'll save money while keeping your infrastructure secure—something all fast-growing SMBs should be looking to achieve.

Harnessing the support of one vendor also means you only have to liaise with a single third party instead of going back and forth with multiple vendors. This issue could cause confusion around which vendor manages what for your business.

> **"A big thing I've heard a lot of applicants talk about, especially from a leadership perspective, is vendor consolidation. The average business probably relies on too many SaaS-based security products and should be looking to adopt a more unified and consolidated security posture."**
>
> – Manuel Osaba, Principal Consultant – Network & Network Security

It also benefits your network recruitment strategy. Rather than searching for and placing multiple people who specialize in network security across various vendors, you could focus your hiring strategy on network professionals who are experts in the vendor you use, such as a network security engineer with a background in Cisco.

Applying the above approaches will help position your business as one that is ready to prevent and combat the various types of network security attacks. Investing in these measures is a short-term commitment that will benefit your organization and the security of your networks in the long term.

With efficient network security processes and strategies in place, your business and employees will feel more secure and comfortable completing daily tasks and upholding daily operations. It will also benefit your client attraction and retention strategies, as companies will be more likely to partner with you if you can reassure them that you can secure and protect their sensitive data, be it email addresses, banking details, and employee information, against network threats.

Of course, to implement any of the above strategies to prevent network attacks, you need people with the relevant skills and experience. This is where prioritizing your network recruitment strategy is important.

SMBS MUST PRIORITIZE THEIR NETWORK RECRUITMENT STRATEGY

We've emphasized in this report that network security is industry-agonistic. Every business needs it, and therefore, every business needs talent with the ability, knowledge, and skills to implement it.

> **"Everyone needs network security. Certain industries are more susceptible to an attack than others, but I don't think you could say network security talent is needed more in a manufacturing company than it is in a law firm or vice versa. I think network security is pretty industry agnostic, and everyone needs it at a certain point."**
>
> – Ben Makepeace, Team Lead - Boston

Most SMBs won't typically have a dedicated network security team. Instead, your security may be managed by an IT director who oversees several verticals across your infrastructure, including network security.
While these individuals may know about network security, they may struggle to implement it effectively due to the other tasks they're responsible for. In such situations, acquiring a network security specialist may be the way to ensure your business is providing sufficient attention to network security.

BUT WHAT NETWORK SECURITY SPECIALISTS CAN YOU HIRE?

You can hire for various network security roles, with talent lending their expertise to specialist and generalist areas of security. Our insight of the 5 Network Security Jobs You Should Consider Hiring For provides insight into the different positions within the space and the skills to look out for in potential hires.

- **Network Security Analyst**
- **Network Security Architect**
- **AI Security Specialist**
- **Network Support Engineer**
- **Network Security Consultant**

You'll also find that many of the professionals you can recruit for within network security specialize in a particular vendor and can have experience ranging from entry-level to senior and director-level.

> **"You can hire the likes of network security engineers, network security analysts, and network security architects. They all deal with network security and will vary in terms of seniority. So analysts, engineers, and architects will go from manager to director-level roles"**

– Ben Makepeace, Team Lead - Boston

> **"More often than not, I feel like I've been recruiting for network engineer job titles that can be network security focused or can be firewall focused, so they could just be called network engineers and not necessarily network security engineers."**

– Jacob Stevens, Consultant - Security

WHAT SHOULD YOU LOOK FOR IN NETWORK SECURITY PROFESSIONALS?

Network security candidates from SMBs often have more diverse skills compared to those from larger organizations due to their experience working across a broader range of responsibilities, making them potentially more adaptable and scalable in their roles.

> **"One thing you could argue is that the applicant becomes more skilled working in an SMB. If an engineer works for a smaller business, they become more well-rounded. Maybe they don't have the level of expertise, but a lot of this is about scalability, too. For example, an engineer who has worked on a network of 100 sites vs. 10,000 sites - obviously, there's a massive difference.**
>
> **If a candidate has developed a broader skill set for managing 100 sites versus someone who has only worked on one specific task in an environment with 10,000 sites, for scalability, most companies would want the person with the 100-site experience and broader skill set."**
>
> – Manuel Osaba, Principal Consultant – Network & Network Security

The quality of a network security engineer is often more important than the specific tools they have used. Skills in areas like firewall management are transferable across different vendors, and any quality engineer should be able to adapt to the different systems of any SMB. While we recognize that SMBs often prefer candidates with experience in the specific vendors they use, like Cisco, Fortinet, or Palo Alto, the core skills surrounding network security are generally transferable.

“I’ve heard a candidate say that firewalling doesn’t come down to the best firewall because firewalling is a skill. Really, it comes down to the engineer. So there’s an idea that you can pick any vendor, but it depends on how good your security engineer expert is.”

– Jacob Stevens, Senior Consultant – Network and Network Security

“We know the skills and experience SMBs typically look for in a network security engineer are vendor-specific, be it Cisco, Fortinet, or Palo Alto experience. It’s normally black and white because the SMB will have already picked a vendor and won’t opt for a multi-vendor environment. So they’ll just need engineers with the vendor-specific skill set.

I’ve spoken to hiring managers before who say network engineers are all the same when you dig below the surface. So, if the candidate has a core skill set, they don’t really mind if they don’t have experience with their specific vendor. For example, if they’re good with firewalls, they’ll be good with firewalls regardless of the vendor or type of firewall because they’re relatively similar; they’re just different jargon and different terminology.”

– Ben Makepeace, Team Lead - Boston

WHAT ARE THE MOTIVATIONS OF NETWORK SECURITY CANDIDATES?

Understanding applicant motivations is key when it comes to network recruitment. Motivations are diverse and change all the time. Professionals who are drawn to network security jobs within SMBs are often concerned about typical aspects of a role, such as pay, benefits and progression. However, they're also influenced by the distance they need to travel, hybrid opportunities and ability to expand their skill set by working on various tasks and utilizing different technologies.

"We recommend to our SMB partners that if they can get someone who's got some experience in the vendor they've selected, they'll benefit from having someone who knows their way around the tool and will get up to speed slightly quicker.

However, SMBs often say it's all about personality and the individual. So if you find someone you like, who you think is a good culture fit, understands the broad areas of technologies, but has worked on a different network security tool, don't be put off by them. Once you get down to it, there aren't that many dissimilarities between candidates who have experience with your specific vendor and those who have worked with other vendors.

Transferable skills and adaptability to work in an SMB environment will be more critical than those of someone who's been siloed in a multinational organization. That's the advice I'd give to SMBs. If you can get someone who knows your specific vendor, that's great. But if you find someone who fits all the boxes but has worked with a different vendor, don't be scared. This person could still be good for your business."

– Martin Rennison, Director of Contracts

WHAT ARE THE MOTIVATIONS OF NETWORK SECURITY CANDIDATES?

Understanding applicant motivations is key when it comes to network recruitment. Motivations are diverse and change all the time. Professionals who are drawn to network security jobs within SMBs are often concerned about typical aspects of a role, such as pay, benefits and progression. However, they're also influenced by the distance they need to travel, hybrid opportunities and ability to expand their skill set by working on various tasks and utilizing different technologies.

"Applicants' motivations change all the time. Do they want to work in a big corporation? Do they want to be able to touch lots of different technologies and lots of different parts of the role? Is that SMB close to home? Does it offer hybrid working? A candidate's motivations to go to an SMB aren't always hemmed into one particular thing and can be completely varied."

– Martin Rennison, Director of Contracts

“Candidates are always going to have different trigger points. If I didn’t know anything about the candidates and I was trying to sell them jobs at SMBs, I would assume they would be attracted to the variety of tasks they would get to do.

For example, I would tell the candidate that you’re not going to be siloed into one job, like solely configuring firewalls or just working on cloud networking. I would tell the candidate that you’re going to get a hand in everything because you’re going to be one of the only people on the network security team. You’ll have the room to explore, expand your skills, and add to your resume.

This variety is a huge draw to many of the technical candidates we work with. Almost all of them say, ‘I want to learn, and I want to grow.’ I feel that probably 70-80% of the time when I’m selling a small business role, I’m telling the candidate about the variety and all the technologies they’ll get to use.”

– Jacob Stevens, Senior Consultant – Network and Network Security

“I think there are two sides to saying you’ll be ‘wearing multiple hats’. I think some candidates think that’s great, but other people see it as being pulled in different directions. It completely depends on the motivations of the candidate. Do they want to work on loads of different things, or do they want to become a specialist in one thing?”

– Ben Makepeace, Team Lead - Boston

CONTRACT VS PERMANENT NETWORK RECRUITMENT

When it comes to hiring network security talent to bolster their defenses, SMBs have excellent flexibility when choosing between contract and permanent recruitment solutions. In this section, our internal specialists provide insight into why a business would opt for contract or permanent services.

CONTRACT RECRUITMENT

Our Director of Contracts, Martin Rennison, perfectly explains why an SMB would consider contract recruitment:

“There are plenty of SMBs out there who don’t know what they don’t know. That’s when bringing in a temporary contract consultant can be really useful. The same solution is ideal if your business doesn’t really want to commit to long-term investment and you don’t know what you need.

You can acquire a contractor for three to six months to support your business with security aspects, such as vendor consolidation and network security assessments. Network security contractors can assess your business, tell you what you need, and help you with the plan you should take and the headcount you’ll need going forward.

This is how you build out a more robust security function. It might be that you upskill your existing IT person, turn to MSP, or do some training and partner with a vendor.

Sometimes, SMBs are frightened about spending time and money on hiring, only for it to go wrong. If you hire a contractor, they can be objective and provide outside expertise. If you've got immediate hiring challenges, you can have a contractor help your business out while you do a more thorough, long-term, permanent search. You also have contract-to-hire or temp-to-perm, where you acquire the contractor, trial them, and if they work out, you can try to hire them permanently.

Overall, the advantages of contracting are that you can often get someone who is a subject matter expert very quickly and is only tied in for a very short period of time. This enables you to upskill your existing workforce while gaining advice that helps your business to grow. It's a short-impact cost, but you'll gain a lot of knowledge in that time that you can use throughout the business."

– Martin Rennison, Director of Contracts

PERMANENT RECRUITMENT

SMBs also have the option to hire network security specialists on permanent deals. Here’s what our experts have to say regarding permanent recruitment:

> **“Particularly with permanent recruitment, smaller companies often hire junior talent and train them. The two routes are either you hire a junior and train them, or you go down the route of contracting where you get someone in for three to six months who can not only do the work but offer some consulting.”**

– Ben Makepeace, Team Lead - Boston

“If you hire junior talent, they can get network security certifications. If you’re working with a vendor, a junior engineer can complete the specific certifications with that vendor.

With SMBs, there may not be enough work for someone to be dedicated to working solely on network security. So, it’s not about the SMB not having the budget to hire someone dedicated to network security. There may just be not enough in the day-to-day job to be doing network security.

An SMB can attract permanent hires by offering them a position that involves some aspects of network security with additional training opportunities. SMBs may hold on to junior hires for three to four years, and when it comes to replacing this talent, the individual and the SMB will have gained more knowledge in network security.”

– Martin Rennison, Director of Contracts

“It can be difficult in a saturated market to attract the very best talent. If you’re going to have high standards for your candidates and you want to compete, it’s very difficult to sell a contract role to an experienced candidate and say: ‘come try us out, but you won’t necessarily have health insurance, you won’t necessarily have your 401(k), and you might not have a job in six months. Some candidates have to be permanent, and they won’t take the job if it’s a contract.”

– Manuel Osaba, Principal Consultant – Network & Network Security

BENCHMARKING YOUR NETWORK SECURITY SALARIES

The salaries of network security professionals vary depending on factors such as the specific job role, seniority, and location. As specialists in network recruitment across the US, we have crafted a list of the typical salaries for security positions.

In this section, you'll find the network security salaries of the roles we recruit for in the locations our team operates, including central Texas, Atlanta, Georgia, Boston, Massachusetts, and New York City. This insight will help you determine the types of salaries and levels of talent you could onboard into your business.

TEXAS

Job Title	25th percentile:	50th percentile:	75th percentile:
Network Security Engineer	$133,000	$162,000	$189,000
Network Security Architect	$158,000	$195,000	$245,000
Compliance Analyst	$60,000	$74,000	$92,000
Security Analyst	$96,000	$123,000	$158,000
IAM Analyst/ Engineer	$106,000	$135,000	$173,000
Cyber/Information Security Engineer	$122,000	$152,000	$195,000
Security Architect	$155,000	$176,000	$198,000
Information Security Manager	$170,000	$215,000	$275,000
CISO - Chief Information Security Officer	$204,000	$247,000	$300,000

GEORGIA

Job Title	25th percentile:	50th percentile:	75th percentile:
Network Security Engineer	$123,000	$150,000	$176,000
Network Security Architect	$160,000	$197,000	$246,000
Compliance Analyst	$60,000	$75,000	$94,000
Security Analyst	$94,000	$120,000	$153,000
IAM Analyst/ Engineer	$106,000	$135,000	$173,000
Cyber/Information Security Engineer	$118,000	$142,000	$179,000
Security Architect	$144,000	$163,000	$183,000
Information Security Manager	$168,000	$209,000	$263,000
CISO - Chief Information Security Officer	$189,000	$229,000	$278,000

MASSACHUSETTS

Job Title	25th percentile:	50th percentile:	75th percentile:
Network Security Engineer	$141,000	$169,000	$198,000
Network Security Architect	$165,000	$204,000	$256,000
Compliance Analyst	$65,000	$81,000	$101,000
Security Analyst	$80,000	$101,000	$123,000
IAM Analyst/ Engineer	$109,000	$155,000	$178,000
Cyber/Information Security Engineer	$119,000	$147,000	$181,000
Security Architect	$178,000	$203,000	$181,000
Information Security Manager	$173,000	$217,000	$276,000
CISO - Chief Information Security Officer	$234,000	$283,000	$344,000

NEW YORK CITY

Job Title	25th percentile:	50th percentile:	75th percentile:
Network Security Engineer	$158,000	$193,000	$225,000
Network Security Architect	$173,000	$213,000	$271,000
Compliance Analyst	$67,000	$84,000	$107,000
Security Analyst	$105,000	$135,000	$175,000
IAM Analyst/ Engineer	$112,000	$144,000	$186,000
Cyber/Information Security Engineer	$130,000	$161,000	$205,000
Security Architect	$160,000	$210,000	$235,000
Information Security Manager	$180,000	$229,000	$296,000
CISO - Chief Information Security Officer	$200,000	$294,000	$357,000

If you require additional information on the above salaries, please get in touch with one of our consultants to see how we can help.

Safeguarding SMBs against network security threats is imperative, given the increasing frequency and cost of cyber and network attacks. SMBs face unique challenges, including misconceptions about their attractiveness to hackers, weaker defenses, human error, and insufficient investment in security measures.

To combat these challenges, SMBs should implement effective network security strategies. These strategies can involve creating disaster recovery plans, making time for employee training, deploying firewalls, using multi-factor authentication and encryption, and consolidating their security vendors.

Additionally, SMBs should prioritize their network recruitment strategy. They should consider both contract and permanent hires to enhance their security posture and ensure they have the right expertise to protect their operations and sensitive data from potential breaches. By implementing these measures, SMBs can take progressive steps to mitigate the risks, safeguard their data, and maintain their reputation in today's tech-driven world.

DISCOVER NETWORK RECRUITMENT EXPERTISE

Knowing which route to go down and who to hire to strengthen your network security defenses is not a decision you should take lightly or one you should have to tackle alone. As experts in contract and permanent recruitment within the network security space, we're best placed to help SMBs reach a decision that benefits their business.

Since 2011, we have been partnering with innovative SMBs, helping them understand and implement the value of network security. Our values of integrity, trust, commitment, and excellence have helped us build long-standing relationships with businesses globally and across the US. With a US headquarters based in Austin, TX, our network recruitment solutions reach Boston, MA, New York, NY, and Raleigh, NC. Our presence allows us to deliver global services to you locally.

Whether you require support in sourcing and placing contract or permanent network security engineers to safeguard your infrastructure or are seeking specialist guidance on how to manage your network recruitment strategy, we can help.

Connect with our team

Martin Rennison
Director of Contracts

GET IN TOUCH

Ben Makepeace
Team Lead - Boston

GET IN TOUCH

Jacob Stevens
Consultant – Security

GET IN TOUCH

Manuel Osaba
Senior Consultant – Cyber & Information Security

GET IN TOUCH

Partner with us today

Contact us today to see how our expertise within the network recruitment space can support your business and safeguard your IT Infrastructure.

www.franklinfitch.com

Franklin Fitch