REPORT

McAfee
Together is power.

Winning the Game

April 2018

Table of Contents

Authors

This report was researched and written by:

- McAfee

Winning the Game

Introduction

Cybersecurity defenses are under unprecedented levels of attack. From old malware foes and newer types, such as ransomware, to sophisticated advanced threats and state-sponsored cyberattacks, breaches are, sadly, now an everyday reality.

It's an ever-changing landscape that organizations face. Take the McAfee Labs 2018 Threat Predictions report.[1] Among its forecasts are an escalating arms race in machine learning as adversaries ramp up their use of artificial intelligence and also a move by cybercriminals to apply ransomware technologies beyond extortion of individuals to higher-value cybersabotage and disruption of organizations.

In the face of these threats, what are the key tools and strategies required to fight back? What are the characteristics and capabilities of those cybersecurity organizations that are better equipped to deal with these threats?

To better understand these questions and explore how organizations are prepared to tackle these cybersecurity challenges, McAfee commissioned market researcher Vanson Bourne to survey 950 cybersecurity managers and professionals in public-sector and private-sector organizations with 500 or more employees in the US, UK, Germany, France, Singapore, Australia, and Japan.

The aim of the research was to gain insight into the key challenges facing IT security organizations in terms of threats, technology investment, and skills and to identify the winning strategies and techniques for fighting back. Areas the survey focused on included:

- The future threat landscape
- Investment plans for the use of automation in cybersecurity defenses
- Cybersecurity recruitment and retention challenges
- Maturity of security operations centers (SOCs)
- Integration of security solutions and vendors into an open platform
- Use of gamification techniques

Connect With Us

1. https://www.mcafee.com/us/resources/misc/infographic-threats-predictions-2018.pdf

The research identifies three clear winning factors to boost the effectiveness of defenses against cybersecurity threats. These are:

- Job satisfaction of cybersecurity employees
- Automation
- Use of gamification

We will explore these findings in more depth in the pages that follow. But first, it is worth briefly examining the key challenges facing organizations today. What exactly is the nature of the game and the battle that needs to be fought?

The Challenges Facing Cybersecurity Organizations

The survey highlights two very familiar security challenges that organizations face in the shape of the growing threat landscape and the cybersecurity skills shortage.

An overwhelming majority (93%) of respondents believe the complexity of threats they will face over the next 12 months will increase and nearly half (46%) admit they will either struggle to deal with this or that threat defense will be impossible (Figure 1).

What is interesting is how organizations are responding to this threat. Hiring more cybersecurity staff alone isn't the answer, given that most organizations already find that difficult. The survey highlights the importance of ensuring job satisfaction to improve retention rates and reduce attrition. As we will explore more later in this report there are some key elements to improving job satisfaction for cybersecurity staff. These range from traditional financial benefits and flexible working arrangements to providing staff the opportunity to work with new technologies such as automation and AI, tackle more interesting work around threat hunting, and take part in cybersecurity gamification exercises. In turn, this can create the kind of cybersecurity environment that is then also more attractive to new recruits.

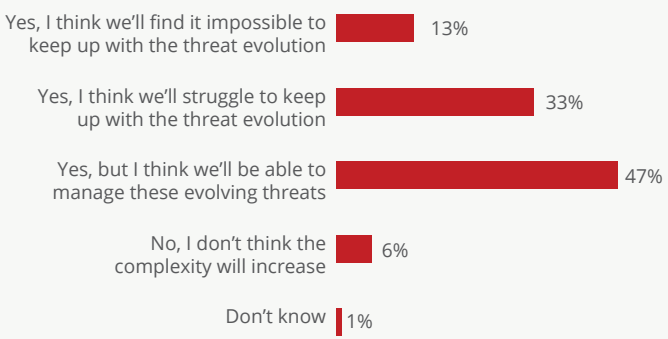

Figure 1. Do you believe that the complexity of the cyberthreats your organization will face over the next 12 months will increase?

Winning Factors in the Cybersecurity Game

1. Job satisfaction of cybersecurity employees

Retaining staff is clearly key in the current climate of a cybersecurity skills shortage and a growing threat landscape. Yet only 35% of survey respondents say they are extremely satisfied in their current jobs and 89% would consider leaving their roles if offered the right types of incentives.

"Nearly half (46%) of organizations admit they will either struggle to deal with the increasing complexity of threats over the next 12 months or that threat defense will be impossible."

Learn more about McAfee's approach to building strong teams and investing in its cybersecurity talent.

Read the blog.

The key factors likely to make people switch jobs are better financial incentives and pay, opportunity for promotion and development, flexible hours, and opportunities to work with exciting new technologies such as automation and artificial intelligence (Figure 2).

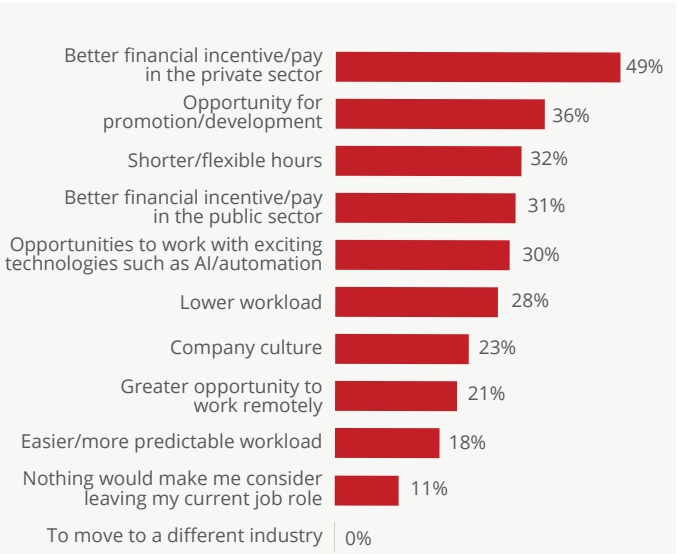

Figure 2. What would be likely to make you leave your current job role?

This retention challenge is further highlighted by the level of churn in many cybersecurity organizations. More than half (52%) of security professionals say the workforce around them is changing regularly, or constantly, every year.

Turnover is a particular challenge as employees become more skilled and therefore more attractive to other organizations. To use a sporting analogy, it's easier to draft rookies and hold onto the longtime veterans. But it's always hard to keep the skilled and in-demand mid-level free agents.

Some organizations believe the only way to win the cybersecurity game is by throwing more people at the problem. This belief is particularly evident among senior managers in the survey who say they need to increase their IT security staff by almost a quarter (24%) to deal with the threats their organizations face.

Yet this seems unrealistic when many organizations still fall short of addressing the requirements of the market. And, shockingly, those who say they find it almost impossible to attract top cybersecurity talent are also the most likely (31%) to report they do not actually do anything to attract this talent.

Key factors for greater job satisfaction

The survey highlights some areas that have an impact on the job satisfaction—and therefore retention and recruitment—of cybersecurity employees. One key factor is the type of work cybersecurity employees are engaged in. The cybersecurity activities that provide respondents with the greatest level of enjoyment (Figure 3) are threat hunting/finding vulnerabilities (55%), resolving threats (55%), and preventing threats entering the network (54%). It's perhaps no surprise that such types of cybersecurity work appeal to many security staff, with just over a fifth (21%) of security professionals saying a threat hunter position either in their current organization or elsewhere is a career aspiration.

On the flip side, those tasks from which cybersecurity staff get low or no enjoyment are the more mundane and repetitive day-to-day monitoring of logs (33%) and

"Respondents who reported greater job satisfaction in their roles considered their organization's SOC to be more sophisticated and automated."

policy enforcement (33%). However, these are tasks that can easily be automated today, potentially freeing up cybersecurity staff to work on more enjoyable, challenging and higher-value tasks that develop new skills. In fact, a quarter of respondents say automation —which we'll cover in greater depth in the next section below—frees up more time for staff to focus on innovation and value-added work, and 21% say it enables staff to research new threats.

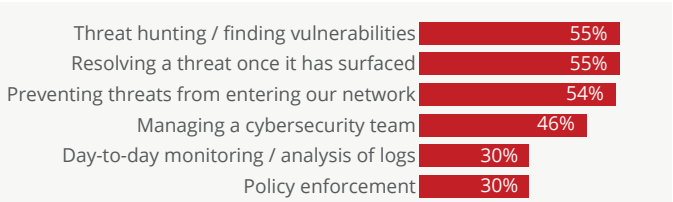

Figure 3a. Which of these activities/tasks do you believe would provide you with the most or a high degree of enjoyment in your job?

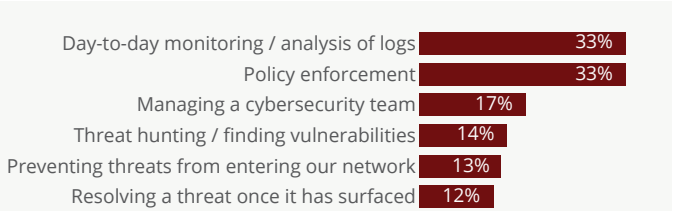

Figure 3b. Which of these activities/tasks do you believe would provide you with low or no enjoyment in your job?

Another factor behind job satisfaction is the use of gamification—which we'll also cover in greater depth later in the report. Those respondents who are extremely satisfied with their jobs are most likely to report that their organization runs games or competitions, such as capture the flag, multiple times per year. And, tellingly, some 80% of extremely dissatisfied employees who report their organization does not use gamification say they wish they did run games such as a bug bounty or hack-a-thon.

A more mature security operations center (SOC) is another marker of organizations with higher job satisfaction among cybersecurity workers. Those respondents who reported greater job satisfaction in their roles considered their organization's SOC to be more sophisticated and automated, with just over a fifth (21%) of those who are extremely satisfied ranking their SOC as "leading."

There is still much room for improvement in SOCs across the board, however. Although 41% of respondents say their organization's SOC is beyond the least mature "initial" stage and at least some way along the spectrum of maturity and automation in the "procedural" stage, only 11% of respondents overall class their SOC as "leading."

2. Automation

As the cybersecurity threat landscape continues to grow, more than 90% of respondents believe threats will become more complex and nearly half say they will struggle to deal with this. This growing threat landscape, combined with the difficulties outlined above that organizations face in retaining and recruiting

"Automation reduces the need for extra staff and frees up existing employees to work on more proactive, enjoyable and value-added tasks that can help in the fight against these growing threats."

cybersecurity talent, means automation is set to become a key element in the cybersecurity game.

Automation in cybersecurity organizations reduces the need for extra staff and frees up existing employees to work on more proactive, enjoyable, and value-added tasks that can help in the fight against these growing threats. And automation also links back to the importance of job satisfaction and the ability to attract and retain cybersecurity talent. Nearly a third of respondents (30%) cite the opportunity to work with new technology such as automation and AI as a key factor that would attract them to a job and influence their decision to move.

Automation also ties in with better integration across the cybersecurity estate. According to the survey, organizations have, on average, eight cybersecurity solutions and seven cybersecurity vendors. With this proliferation of solutions and vendors, just over three-quarters (76%) of respondents agree that their organization's cybersecurity would be much safer if they implemented an open platform for integrating all of their security solutions from multiple vendors.

Automation investment priorities

What is the current picture for the adoption of cybersecurity automation technologies (Figure 4)? Most organizations (92%) say they are already using some form of automation in their cybersecurity processes. However, much of that appears to be at a very basic level and automation is not being used as effectively as it could be, with much room for improvement. For example, use of automation is still relatively low for key cybersecurity tasks such as identifying all locations of a threat (29%), correcting and remediating threats (33%), detecting threats across some of the IT architecture (33%), and threat containment (36%).

However, automation is clearly set to be a key pillar of safer and more effective cybersecurity organizations in the future. A majority of respondents are already investing or planning to invest in cybersecurity automation, and 62% of those who currently aren't say they plan to do so in the next three years. Less than a quarter (24%) said they have no plans to invest at all. Of the small numbers not planning to invest in automation for their cybersecurity defenses, almost a third (32%) say a lack of in-house skills is the main reason for this decision.

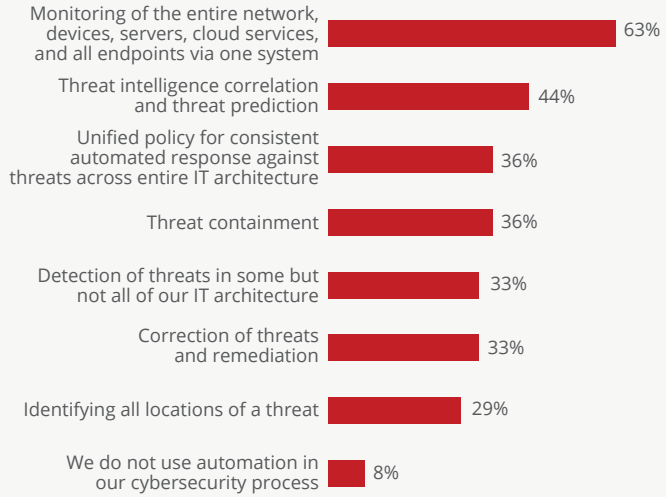

Figure 4. Which of these areas of the cybersecurity process is your organization using automation in?

"76% of respondents agree that their organization's cybersecurity would be much safer if they implemented an open platform for integrating all of their security solutions from multiple vendors."

The top three priority areas for investment in automation—among those who are already investing or plan to in the next three years—are threat detection (52%), threat intelligence (40%), and training for both 'on-the-ground' staff (39%) and high-level staff (37%) to better work with automation tech.

Automation benefits

There are proven benefits of automation in cybersecurity (Figure 5), with almost all (99%) of those using automation saying they have seen benefits. These include increased efficiency (50%), greater visibility

Figure 5. The benefits experienced by respondents' organizations that already use automation in cybersecurity defenses.

THREE PILLARS OF CYBERSECURITY AUTOMATION

1. Integration

Integrating detection and response systems is an essential part of automating the cybersecurity environment to help employees deal with the volume of information and identify the pieces that matter. The open source OpenDXL initiative, which is sponsored by McAfee, provides an easy way for organizations to integrate cybersecurity technologies.

2. Security information and event management (SIEM)

An SIEM product has continuous access to a data feed from across the cybersecurity estate. It analyzes areas such as DNS data, perimeter firewalls, and VPN traffic. It can be configured to identify suspicious patterns or activities on the network and carry out immediate automated historical analysis. This not only aids detection but can speed up incident response times, potentially mitigating the damage to data and systems from any breach.

3. Machine learning

In relation to cybersecurity, machine learning is changing the game within corporate environments managing massive amounts of data. Although some actions may need to be managed through human intervention, machine learning can take care of much of the easy and predictable work. For example, it can be used to set correlation rules to make the same review decisions you make on a routine basis, and then set alarms, create watch lists, or use scripts to package and forward data. With machine learning, you can automate advanced classification, scoping, and prioritization of security events, making it possible to perform both predictive and prescriptive analytics.

(46%), reduced threat detection time (42%), and cost effectiveness (40%). And 81%—an overwhelming majority—of respondents believe that their cybersecurity would be much safer if they implemented greater automation.

3. Use of gamification

Gamification is growing in importance as a tool to drive a better-performing cybersecurity organization. Four in 10 organizations say they already organize some kind of gamification exercise at least once per year. The most common is capture the flag, followed by red team versus blue team.

Benefits of gamification

Almost all (96%) of those using gamification say they have seen benefits. The top benefits of gamification (Figure 6) are raised awareness and knowledge among IT staff of how breaches can occur (57%), how to avoid becoming a victim of a breach (49%), and how to best react to a breach (46%); it also enforced a team work culture necessary for quick and effective cybersecurity (43%).

Figure 6. The percentage of respondents who believe gaming techniques and concepts have encouraged stronger cybersecurity defenses.

Significantly, these benefits of gamification are recognized by top management and not just security professionals, with 77% of senior managers agreeing that their organization's cybersecurity would be much safer if they implemented more gamification.

However, there is huge room for improvement in the use of gamification as a tool to win the game. Despite the benefits achieved and the fact that even 81% of those not currently using gamification believe there could be benefits, between one fifth and one half of organizations don't play any games at all. At McAfee, we consider gamification activities as a critical part of our on-going development for our cybersecurity teams and run table-top exercises every two weeks, and red team exercises monthly.

Job satisfaction and gamification

As we touched upon briefly earlier in this report, there is also a correlation between the use of gamification and higher job satisfaction among cybersecurity staff. If we look at the most popular game, capture the flag, more than half (54%) of respondents who are extremely satisfied in their roles say their organization uses this

"Almost all (95%) of those organizations using gamification say they have seen benefits."

gamification technique once or more a year, compared to just 14% of those employees who are dissatisfied in their roles.

This correlation becomes even more apparent when we look at it from the perspective of those not running games: here, respondents who are dissatisfied in their jobs are far more likely (around 7 in 10) to be working in organizations not running cybersecurity games at all compared to those who are extremely satisfied (around 4 in 10). And 80% of extremely dissatisfied employees who report their organization does not use gamification say they wish they did run games.

Video gamers—The next generation of threat hunters?

Could one answer to tackling the cybersecurity skills shortage and fighting new and ever more complex cybersecurity threats lie outside the typical cybersecurity hiring profile in a generation entering the workforce who have been brought up on video and computer games?

When we look at current cybersecurity employees, almost half (45%) of cybersecurity professionals are estimated by respondents to be frequent or experienced video gamers, according to the survey responses.

An overwhelming majority of respondents (92%) also said gamers possess skills that make them suited to a career in cybersecurity. And three-quarters of senior managers say they would consider hiring a gamer even if that person had no specific cybersecurity training or experience.

Gamers quickly learn to continually look for clues, tools and weapons in their quest for success. And they develop persistence, endurance, observation, and logic. This is supported by the survey, which suggests that gamers have many of the core skills that cybersecurity threat hunters of the future will need. More than three quarters (78%) of respondents say the current generation entering the workforce, who have been raised playing video games, are stronger candidates for cybersecurity roles than traditional hires.

According to the survey respondents, the top skills gamers bring to cybersecurity are (Figure 7):

- Logic
- Perseverance
- An understanding of how to approach adversaries
- A fresh outlook compared to traditional cybersecurity hires

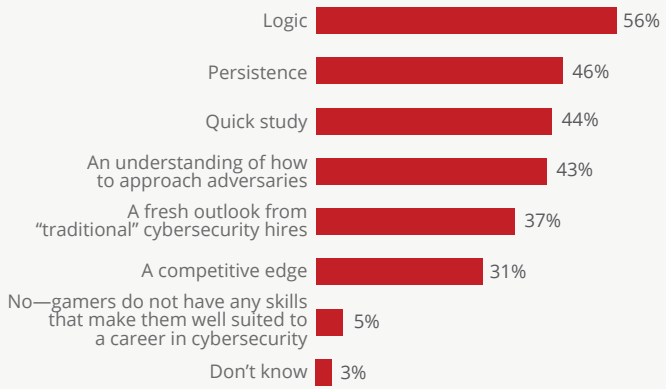

Figure 7. Do you believe that gamers possess any of these skills that make them well-suited for a career in cybersecurity?

"Three quarters of senior managers say they would consider hiring a gamer even if that person had no specific cybersecurity training or experience."

Given those skills, it's perhaps not surprising that 72% of respondents say hiring experienced video gamers into the IT department seems like a good way to plug the cybersecurity skills gap.

Summary

Just as taxes and death are often said to be the only two certainties in life, a growing cybersecurity threat landscape and a skills shortage are ever-present challenges for IT organizations.

There is cause for optimism, however. Most organizations have plenty of room for improvement in tackling these challenges. In short, there are ways to fight back.

Many security managers believe the only way they can try to keep ahead of the growing threat landscape is to hire more staff. Not only is this unrealistic given the high turnover of cybersecurity staff and the difficulty of attracting new talent, but it ignores far more effective ways of detecting and responding to incidents using automation.

Adoption of automation in cybersecurity appears to still be at a fairly basic level, yet the research shows there are proven benefits, and most respondents agree that greater use of automation would make their cyber defenses safer. It also addresses the challenge of staff retention by freeing up employees from routine tasks such as policy enforcement to spend more time on the value-added and enjoyable tasks such as threat hunting. Working with technologies such as automation and AI is also one of the key factors likely to attract employees to a role.

Many organizations are also falling short of offering the right kinds of incentives to retain and attract staff. A majority of organizations (84%) report some element of difficulty in attracting top talent. However, those respondents who say their organization finds it almost impossible to attract top cybersecurity talent are also the most likely to admit they do not actually do anything to attract this talent. And only around a fifth of those respondents say their organizations offer incentives such as training opportunities, flexible working, and the chance to use new technologies.

Given the high levels of staff churn at many organizations, it is also more important than ever for senior managers and HR departments to consider alternative methods to plug this cybersecurity skills gap. For example, the research singles out video gamers—even those without a background in cybersecurity—as people who have the right types of skills and a much-needed fresh approach to threat hunting compared to traditional security hires.

Finally, there is scope for far greater use of gamification by IT organizations. Again, the research shows there are proven benefits of playing more games such as capture the flag in terms of improving cybersecurity practices by increasing awareness and knowledge and creating a better team work culture.

"72% of respondents say hiring experienced video gamers into the IT department seems like a good way to plug the cybersecurity skills gaps."

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com