Symantec

High Alert Series
Chapter 1: Perfect Storm

High Alert: Tackling Cyber Security Overload in 2019

Understand the impact of patchwork defenses and start your journey to reduced complexity >

Inside this edition of High Alert

Exclusive new research conducted on behalf of Symantec draws back the curtain on cyber security to reveal an industry in crisis. CISOs and security teams feel outgunned by cybercriminals, a step behind the pace of technological change, and overwhelmed by alerts. Worst of all, security professionals everywhere feel they're living on borrowed time as reports of burnout rise. Not only is this constant state of high alert increasing stress. According to a leading psychologist, it's dramatically heightening the risk of major cyber security incidents.

It's time for change.

What is the High Alert series?

Based on the opinions of over 3,000 security decision makers in the France, Germany and the UK, with analysis from CISOs and Dr. Chris Brauer, Director of Innovation at Goldsmiths, University of London, the High Alert series lays bare the real state of cyber security in 2019 – and what you can do to regain the initiative.[1]

Across four chapters, we'll explore a different cyber security topic. Combining insights, analysis and recommendations, you'll learn how your organisation can master cyber security for the cloud generation: protecting your reputation, sustaining customer trust, guarding against financial penalties, and balancing budgets and resources.

Building over the coming months, the High Alert series will address four topics:

- **High Alert Chapter 1: Perfect Storm**
- **High Alert Chapter 2: Skills Crisis**
- **High Alert Chapter 3: After the Breach**
- **High Alert Chapter 4: Secure Enablement**

Alongside new intelligence and analysis, you'll learn how cyber security industry leader Symantec offers an alternative approach to help you cut through today's cyber security chaos.

1 Research conducted by Symantec in collaboration with Goldsmiths, University of London and research consultancy Thread. Surveys were distributed in Winter 2018/19 to 3,045 individuals across France, Germany and the UK. Quantitative study figures for Germany and France are from Censuswide; UK figures from YouGov. See back page for more information.

Contents

1 Perfect Storm: cyber security now

Cyber attacks are more sophisticated and capable than ever before. For most of the population major breaches and exploits are the stuff of news headlines. But for cyber security professionals, today's aggressive threat landscape is a daily reality. Their mission? Addressing seemingly endless attacks from an increasingly professional, well-funded, highly motivated and experienced array of adversaries.

As cyber security professionals work to face down this evolving threat landscape, they do so short of qualified personnel and in the face of wide gaps in strategic and operational information sharing. For cyber security decision makers, these challenges are felt at a deeply individual and personal level.

Cyber security: the psychological impact

A career in cyber security requires focus, extreme attention to detail, creative problem solving and rational decision-making in high-pressure scenarios. But with increasing regulation, better-equipped attackers, growing complexity of the digital estate and thousands of alerts going off at the same time, security leaders are overloaded. This overload can have a serious impact on their ability to make sound decisions.

Sensory overload, fatigue and stress impair memory[2], disrupt rational thinking and negatively impact every cognitive function we have[3]. Studies show that when you're stressed, signals in the brain associated with factual memories weaken, while areas in the brain associated with emotions strengthen[4]. Whilst the human brain is adept at many things, dealing with vast quantities of information and alerts can hamper our cognitive function[5]. The more information and alerts we receive, the more numb we become to them.

> *Even just the anticipation of stress can impact cognitive function throughout the day. A study from Penn State showed those who woke up feeling as though the day ahead would be stressful experienced problems with working memory; a function which helps people learn and retain information even when they're distracted. Researchers say the anticipation of stress impacts cognition, even if a stressful event does not occur.*
>
> Penn State 'Experiencing a Stressful Day May Lower Cognitive Abilities Throughout the Day.' Neuroscience News, 3 July 2018.

2. "Stressed Memories: How Acute Stress Affects Memory Formation in Humans". Journal of Neuroscience. & Peavy, 12 August 2009. "Effects of Chronic Stress on Memory Decline in Cognitively Normal and Mildly Impaired Older Adults". American Journal of Psychiatry. 15 September 2009.
3. Everyday Stress Can Shut Down the Brain's Chief Command Centre, Scientific American, April 2012.
4. Our Brain on Stress: Forgetful & Emotional, psych central, 8 July 2018.
5. The Overflowing Brain: Information Overload and the Limits of Working Memory, By Torkel Klingberg, Oxford University Press, 2009.

Symantec wanted to better understand the impact of these pressures on the cyber security industry. How do security leaders view their industry and their workloads? How do they see the threat landscape changing? And how well equipped do they feel to deal with bad actors infiltrating their networks?

In collaboration with Dr. Chris Brauer and Goldsmiths, University of London, Symantec surveyed over 3,000 security decision makers across three countries – France, Germany and the UK. The aim was to gain real insights from those at the coalface.

The picture painted will be both poignant and familiar to readers within these roles, but it also raises an important fact: the industry cannot afford to continue like this.

Navigating the perfect storm

Security leaders are overwhelmed. Two thirds of cyber-security decision makers (65%) feel they are being put in a position where they are set up for failure. Additionally, 82% report feeling 'burnt out', 63% think about leaving the industry, and 64% think about quitting their job (figure 1).

But the overwhelming workload and pressure of the role doesn't seem to deter them from the mission. Most security leaders appear to be adrenaline junkies; fully immersed in their work, and its potential to make a difference, even when it's stressful (92%). Security leaders tend to be motivated by high-pressure situations and find their work environment thrilling, even though it's challenging (figure 2).

Figure 1: Cyber security professionals feel overwhelmed

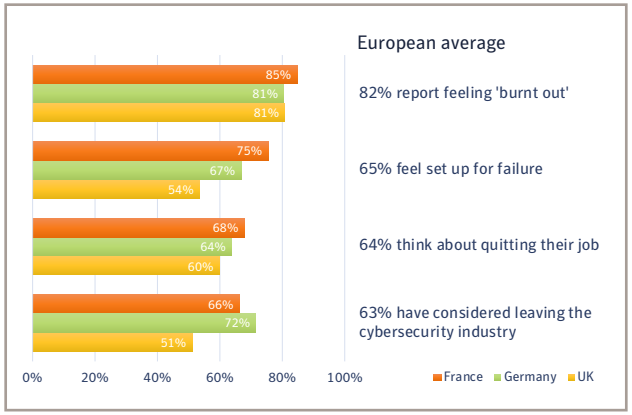
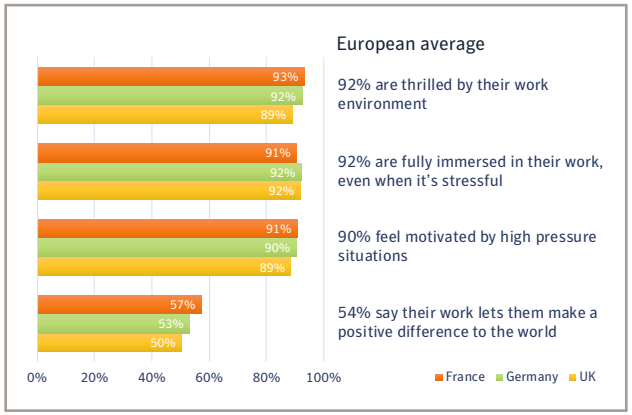


Figure 2: Cyber security is a vocation



> *Stress dramatically impacts our ability to make good decisions. It impairs your memory, disrupts rational thinking and negatively impacts every cognitive function you have. In an industry like cyber-security, which requires focus, creative thinking, attention to detail and rational decisions in high pressure scenarios – stress can be crippling. Highly stressed workers are far more likely to be disengaged and ultimately quit. In an industry already suffering a skills shortage, this kind of stress can present a significant risk.*
>
> Dr Chris Brauer, Director of Innovation, Goldsmiths, University of London.

Cause and effect

But what is causing the sense of overwhelm that so many professionals in the industry are feeling? According to the research, there are numerous causes, but four stand out.

1. Increasing regulation

The leading source of strain for cyber security leaders is government regulation. Four in five (86%) reported that mounting regulation, such as GDPR and the NIS Directive, was increasing pressure in their role. Two in five reported concerns that they would be held personally liable for a data breach.

2. Attackers gaining ground

The second biggest issue is the rise of the adversary and an increasing volume of threats and alerts. The level of sophistication, motivation and organisation in cyber-crime today is more comparable to mature enterprises than to the stereotype of the hooded lone hacker. Attack groups are agile and persistent, continually probing for weaknesses and moving swiftly to exploit those they discover. Some 82% said that having 'too many threat alerts to deal with' was increasing the pressure in their role. Just over half (55%) feared dismissal if a breach happened on their watch.

3. Growing enterprise complexity

The size and complexity of the estate defended is also increasing pressure. Whether through digital transformation, merger and acquisition, an increasingly connected and distributed workforce, or simply a question of scale – the attack surface is expanding.

Four in every five (82%) of security leaders agreed that having to secure too much data in too many places is making the job more stressful, costly and complex.

Figure 3: Cyber security's technology challenges

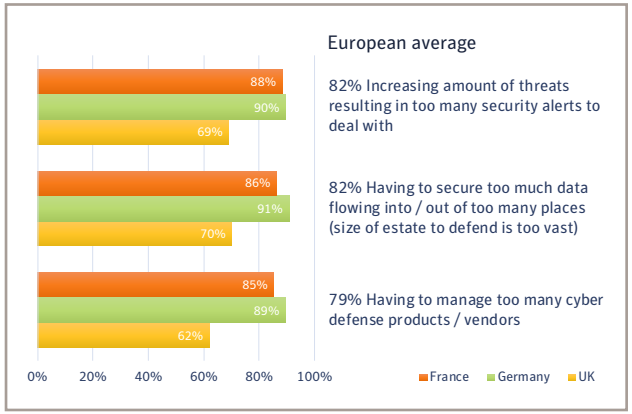
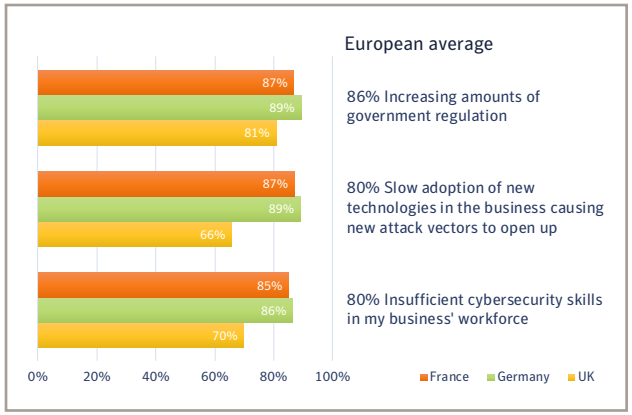


Figure 4: External and cultural challenges



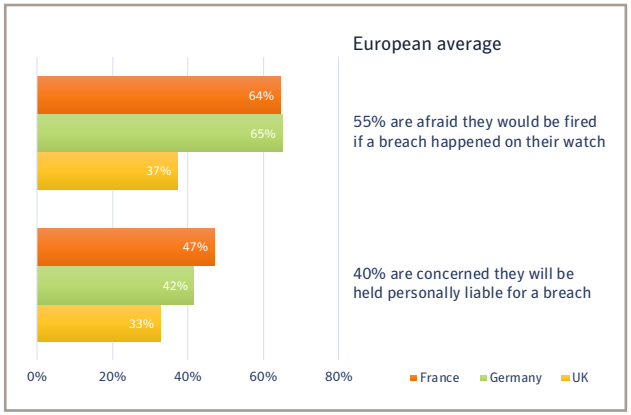
In mature organisations, cyber defenses have often grown piecemeal over time. Simply maintaining legacy defense technology is a significant burden.

4. The ever-present skills gap

Four in every five (80%) reported that insufficient skills in their workforce is causing increased pressure. In many cases, the existing base of experienced cyber security professionals has been 'outdated' by the rise of cloud and mobile. Almost half (48%) of respondents believe attackers now have the skills advantage over the defenders (figures 3 & 4).

These challenges are not only adding to the stress felt by security professionals (figure 5), they are also making it more difficult for them to keep their business safe.

Figure 5: Cyber security professionals feel vulnerable

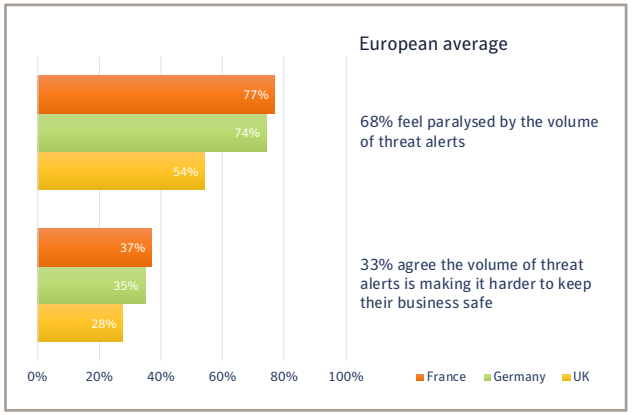


Security infrastructure sprawl

There's a certain degree of irony that efforts to protect the enterprise are also increasing stress. 79% reported that managing 'too many cyber defense products or vendors' was increasing the pressure within their role.

Multiple security products and services generally means a large number of alerts – all coming from different places. And there's only a finite pool of people within an organisation that can review and resolve these. Two thirds (68%) of cyber-security decision makers said they'd felt 'paralysed' by the overwhelming volume of threat alerts. A third (33%) reported that threat alerts, designed to help keep a business safe, are making the situation worse due to their sheer volume (figure 6).

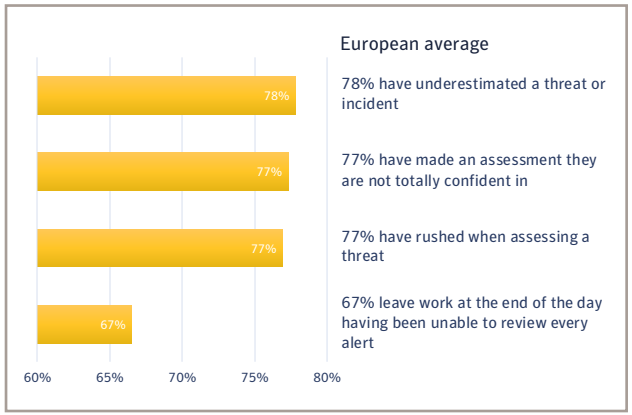
Figure 6: Cyber security suffers from information overload



In the face of such huge workloads, the majority of those questioned (67%) said their cyber security teams left work at the end of the day with threat alerts left unreviewed. The volume appears to be impacting the security of enterprises. Already 41% of security leaders believe a breach is inevitable. A third (32%) say their organisation is currently vulnerable to avoidable cyber security incidents. A quarter (26%) admitted they have already suffered one of these.

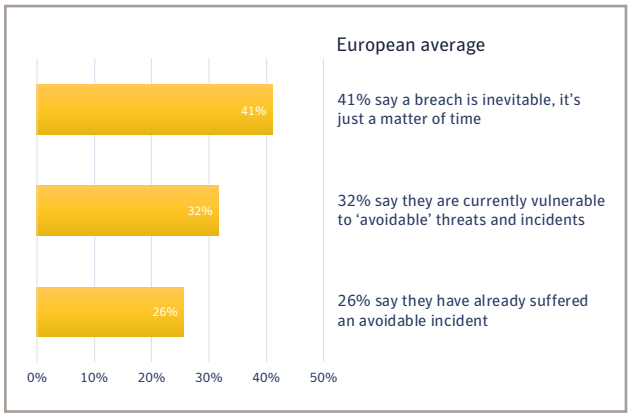
This sense of being overwhelmed is having an impact on their role (figure 7).

Figure 7: The impact of cyber security overload



Quantity certainly isn't the answer when it comes to security services. But if the answer lies in quality, many security leaders feel under-resourced and ill-equipped to provide it (figure 8) – particularly with attackers becoming increasingly savvy.

Figure 8: Attitudes towards cyber security risks



Now what?

In an increasingly broad and capable threat landscape, how do cyber security leaders move out of a state of personal overload? The answer lies in moving from a reactive and fragmented model, to a consolidated and strategic one. Yet to invest the time, energy and resource into defining and executing against a cyber security vision, they must first regain control of the finite human resources such an approach would free up.

One of the biggest factors at play here is the overhead that goes into managing a patchwork of IT security vendors across a vast, rapidly evolving IT estate. A patchwork approach to cyber defense creates vulnerabilities and overburdens cyber security teams.

This tension is underpinning a push towards simplicity and integration across the industry; fewer vendors, less complexity, and more centralised management. With this transformation, the cyber security industry is entering the platform era.

An open standards security platform, such as Symantec's integrated cyber defense (ICD) platform, gives a modern foundation on which to build. It integrates security data feeds, cutting duplication, improving accuracy and speeding decision making. With the ICD platform, security leaders can add new security solutions as required (typically cloud-centric ones such as CASB and cloud workload protection) and feel safe in the knowledge they will integrate quickly and easily into the ICD platform. The ICD platform's automation capabilities mean that new solutions won't require time-intensive manual patching and maintenance, or the manual integration of new data sources into reporting and compliance workflows.

With these capabilities, it becomes far easier to hand selected functions off to managed services. In an industry with a severe skills shortage, an integrated platform enables cyber security professionals to minimise mundane tasks in favour of adding more value through proactive, higher level work.

A pathway to protection

There is much for you to consider as part of this approach, but four of the most fundamental elements are:

- Mature and consolidate cyber defenses by adopting a platform approach, automating key processes and compliance
- Educate the business on the threat landscape, and demonstrate how cyber security can become a business and transformation enabler
- Be both pragmatic and bias conscious in your efforts to overcome the skills gap – recruit and up-skill a diverse range of talent to tackle the multiple challenges you face
- Define your organisation's risk posture, securing buy in and 'sign-off' from specific business departments and the board.

With skilled talent, the right processes and tools, it is possible to evolve your roles from overloaded and reactive, to confident and strategic. In subsequent chapters of this research series, we'll explore some of these key factors in how you can work towards overcoming this state of overload.

> *"The current patchwork approach to security tooling and strategy is creating more problems than it solves. There is so much daily noise that it's near impossible to work out what is most important. Meanwhile the overlaps and chinks between defensive systems present hackers with new opportunities for exploit. The volume of alerts, the constant patching, and rapid emergence of new threat vectors, are absorbing the attention of security professionals, leaving little time for a more strategic approach."*
>
> Darren Thomson, CTO EMEA, Symantec

Watch the High Alert Summit webinar

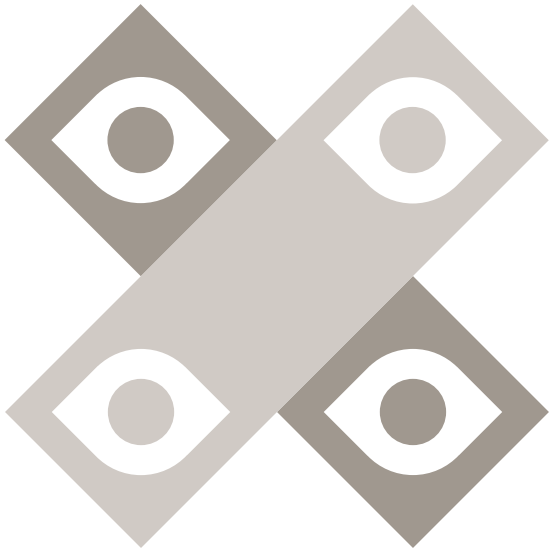
Join Darren Thomson and Dr Chris Brauer, Director of Innovation at Goldsmiths, University of London, as they analyse the High Alert Chapter 1 findings and recommend how to reduce your own cyber security complexity.

REGISTER FOR THE WEBINAR NOW

Summary and next steps

If you want your organisation to reduce cyber security complexity, and enjoy proactive, holistic protection with a reduced management burden, it's easy to get started with Symantec Integrated Cyber Defense.

We'll work with your cyber security specialists and partners to complement, streamline and ultimately transform your existing security infrastructure at a pace that suits your organisation.



Choose Symantec with confidence

Industry analysts consider Symantec a market leader in information security. The products that comprise the Symantec Integrated Cyber Defense are individually recognised as among the best in their fields:

- Symantec Secure email Gateway was named a Top Player by The Radicati Group
- Symantec was named a Leader for the 11th year in Gartner's Secure Web Gateway Magic Quadrant
- Symantec was named a Leader in the Gartner CASB 2018 Magic Quadrant
- Symantec was named a Leader in Forrester's Zero Trust Wave Report 2018

Next steps

Watch out for the High Alert series Chapter Two, Skills Crisis, **coming in May**.

Learn more about simplifying cyber security complexity with the Symantec Integrated Cyber Defense Platform.

VISIT WEBSITE NOW

About the Research

The High Alert research study was conducted by Symantec in collaboration with Dr Chris Brauer, Director of Innovation, Goldsmiths, University of London and research consultancy Thread. The research was directed by Dr Chris Brauer and Dr Jennifer Barth and led by Sean Duggan. The German and French figures for the quantitative study are from Censuswide; the UK figures are from YouGov.

Survey fieldwork was undertaken in Winter 2018/19. The research used quantitative methods to measure, define and distinguish the experiences of cyber-security professionals in leadership roles in three countries: France, Germany and the UK. The survey was distributed to 3,045 individuals across France (1,002 respondents), Germany (1,003 respondents) and the UK (1,040 respondents) in middle or upper leadership roles, with decision making involvement in cyber security.

Symantec