IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The CISO's Next Priority isn't Technology – it's Building a Great Employee Experience

Leon Ward

Leon Ward
Vice President of
Product Management
ThreatQuotient

Biography

Leon Ward is the Vice President of Product Management, ThreatQuotient (https://www.threatq.com). With over 15+ years of experience in information and network security, Leon leads product aspects of ThreatQuotient's innovative threat intelligence platform, ThreatQ. In this role, Leon drives the ThreatQ product roadmap aimed at improving the efficiency of analysts, security teams and threat operations.

Prior to ThreatQuotient, Leon was Cisco's Group Product Manager of Security Innovation, contributing to a number of exciting product launches that were aimed to change the infosecurity world. Leon was previously a Director of Product Management at Sourcefire, where he managed the detection capabilities in the company's line of network products (SNORT).

Leon blogs at https://www.threatq.com/resources/

Keywords CISO, Employee Experience (EX), Cybersecurity, Automation, ROI (Return on Investment (ROI), Wellbeing, Inclusion, Security automation, Human Resources (HR)
Paper type Research

Abstract

Qualitative research highlights the importance of training and development in both attracting and retaining employees. However, once staff achieve new qualifications or certifications, their skills become more valuable, and they may seek – or be approached for – higher paid roles elsewhere. Keeping valuable IT staff now relies on giving better employee experience (EX), explains the author of this article.

Introduction

In security, we are very used to talking about features and functions in the tools we use. When it comes to measuring the positive impact of what we spend on cyber, in terms of both people and equipment costs, we tend to be equally abstract – for years, 'mean time to detection' and 'mean time to resolution' have probably been the two most widely-used metrics for cybersecurity progress, and measuring the number of security incidents handled is still probably how the CISO tracks his team's contribution to the organization.

But no longer. Today we need to start thinking about measuring cyber's impact in completely new ways – or to be more accurate, concepts new to us in IT security but already very familiar to our colleagues in HR; with terms that seem very far from threat intelligence, such as wellbeing, inclusion and creating psychologically safe spaces.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

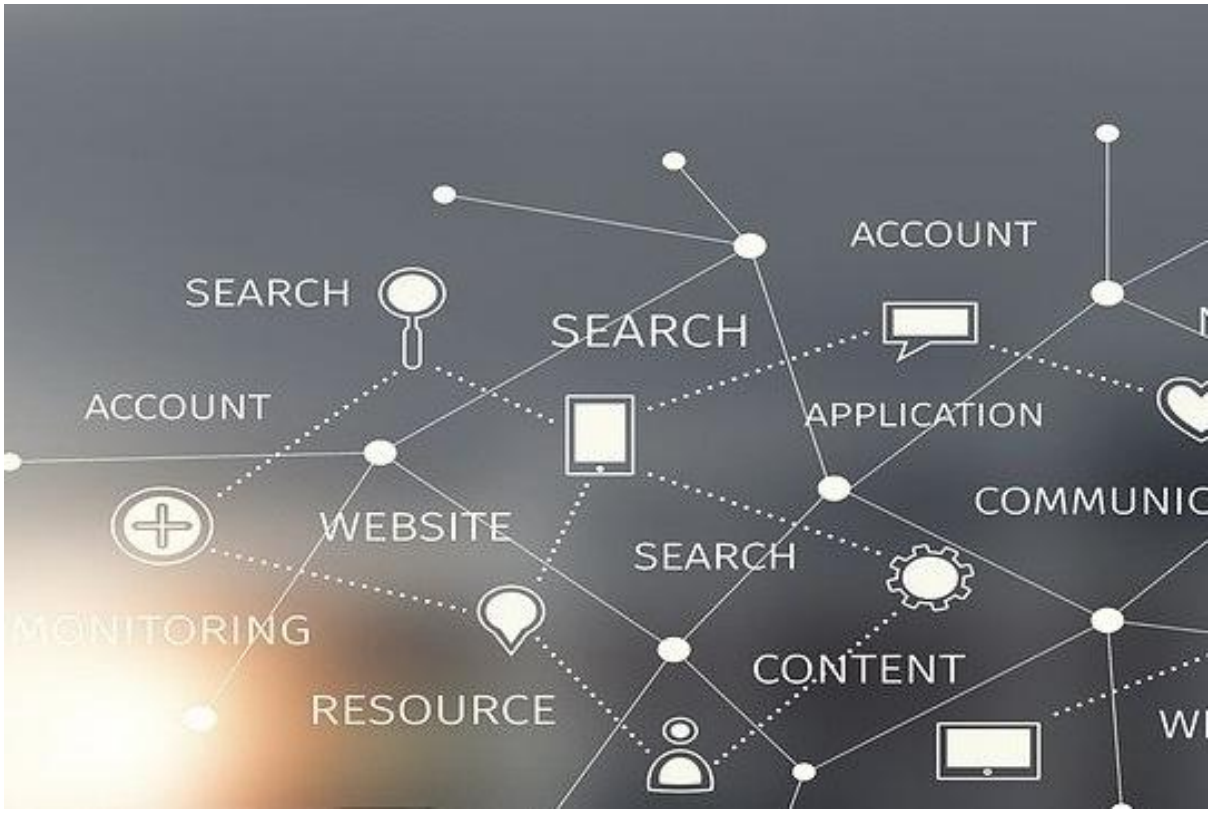
Why 'EX' is becoming more important

In non-IT parts of the workplace, the shorthand for such approaches and employment policies comes under the umbrella term 'EX' – employee experience – which has been defined by Gartner as the way in which employees internalise and interpret the interactions they have with their organization[1], as well as the context that underlies those interactions.

What makes the extension of CISO thinking into this area even more remarkable is that it's in the context of cybersecurity automation – defined as the provision of real-time detection, rapid response, and proactive defence tools, so making systems that can help protect us at scale and which optimize many of the routine tasks human security practitioners get asked to do.

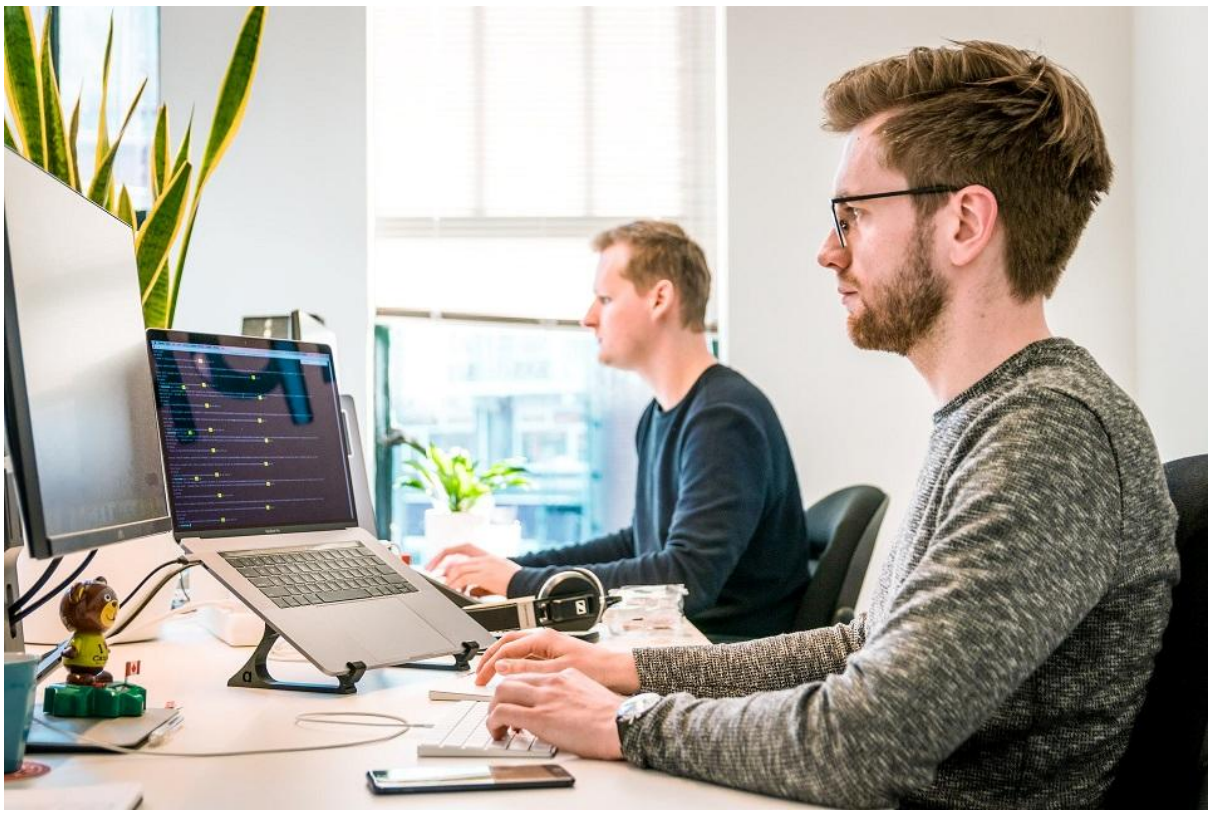
Security automation is still a relatively new part of the wider cybersecurity armoury, which explains why it's not as big a spending priority for Chief Information Security Officers (CISOs), as other cyber tools with 2023 market size of $9 billion (though set to grow to $17billion by 2028)[2]. However, interest is rapidly rising, as we start to see how we need to be able to operate at cloud-level scale and machine learning speed to cope with the evolving sophistication of security threats.

So far, it's been hard to measure security automation return on investment (ROI). I can measure ROI by automating workflows in a business process; tasks are completed faster and cheaper. But if automation just keeps everything going without interruption, is that enough of a Key Performance Indicator (KPI)?



IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**



Is the real ROI for a tech product how good it makes the user feel?

Well, now we have a better KPI. For the last three years, here at ThreatQuotient we have been polling cyber teams about their experiences, and this year we talked to 750 senior cybersecurity professionals in the UK, U.S. and Australia from big organizations in verticals from central government to retail and financial services.

We found lots of interesting statistics, but for the first time we found respondents putting the HR and people side of cyber ahead of other aspects. This starts with the top three challenges facing cybersecurity teams being framed as insufficient budget, growing regulatory and compliance challenges – but also high team churn rates. Even more strikingly, employee satisfaction and retention has become the main metric for assessing cybersecurity automation ROI for more than 60% of the survey respondents – outweighing those older 'mean time to resolution' measures we have always utilized.

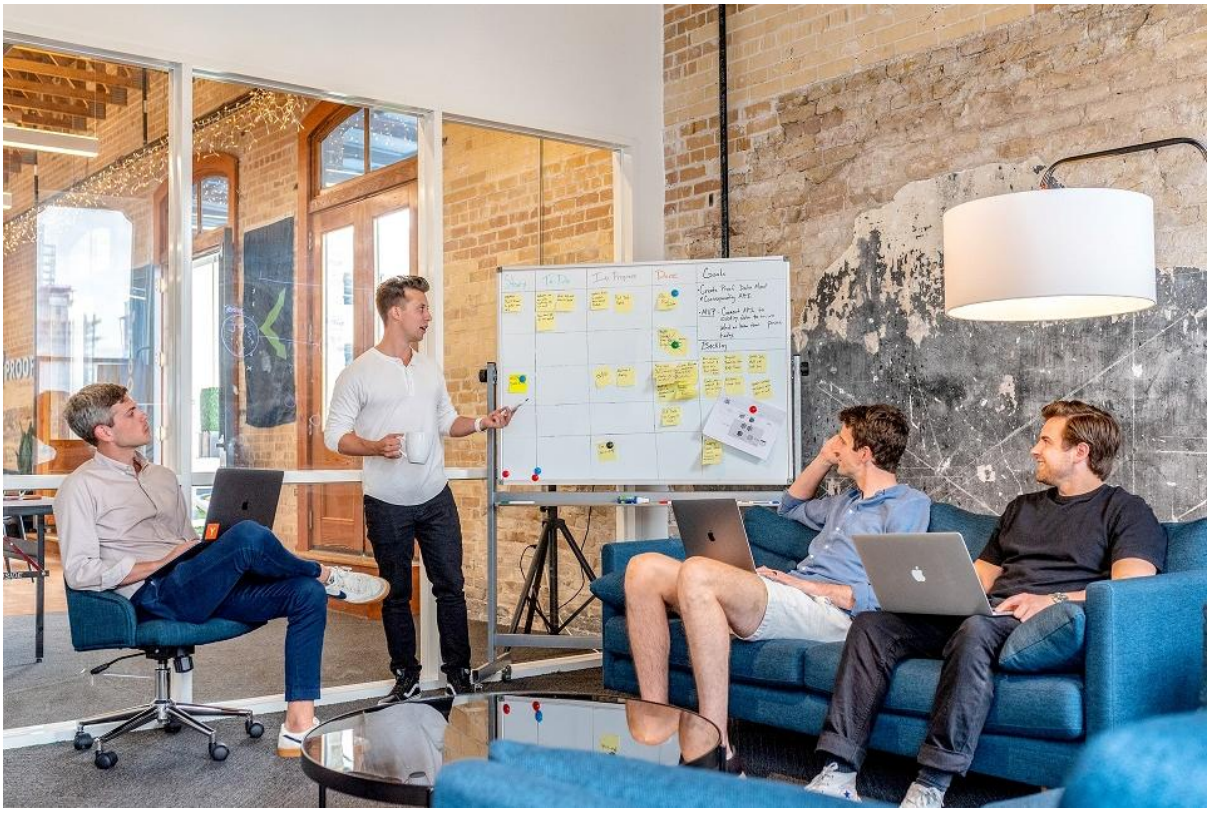
So, the point of investing in cybersecurity automation is becoming less the straightforward technical and security protection measures. Now, it's to get automation in to help with making the analyst's job easier and so more enjoyable. By getting the computer to shoulder the burden of low value/repetitive activities and release the skilled professional to take on more interesting and fulfilling work. In strict security terms, think about how nice it would be to not have to click the same eight buttons repeatedly to achieve your outcome, or for it to be easier to work through that bunch of domain names which have been incorrectly blocked that you receive every day.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

But from what I'm seeing in the sector, it's not just automation of this kind of work that the CISO is looking for help with here. Across multiple industries, companies are now actively looking to improve employee satisfaction, to consciously see how their wellbeing can be boosted, and reduce churn. Personally, I see a lot more change at senior level; it used to be you would see the same head of security in a job for five to ten years, but since COVID and us all re-examining what we want from work, people now seem to move or even leave the sector every two to three years instead.

Security leaders also want better Learning and Development (L&D) for their people. We asked what the top three most desirable aspects of a new cyber automation product was; training availability – so making sure people can actually get value out of the product and the technologies they are deploying – came in at a strong second (23%), just behind if the tool can integrate with multiple data sources (24%). But I also hear a lot of employers talking highlighting support for hybrid working, diversity, flexibility around parenting in their recruitment campaigns – all classic EX concepts that suddenly make sense in this area of tech, too.



Time for our tech culture to get more welcoming and supportive

There's a kind of fascinating contradiction here; by making automation mainstream, we've also realized that making routine work simpler has exposed a much bigger issue around what we are asking our analysts to do all day – and the security leader has taken notice.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Of course, there's an EX message in our results here that's not just for the security or enterprise IT leader. It's also for makers of security products in general. Do cyber vendors need to incorporate the human benefits of their solution into their product design and messaging, and not focus strictly just on the bits and bytes?

I think the answer is clearly yes. While some sceptics may dismiss all this as 'fluffy,' the reality is that we simply can't afford to ignore the people side of our business anymore. When observers speak with genuine concern that the UK's cyber security skills gap is 'a ticking time bomb'[3] for the whole economy – and the government is openly saying the people in charge of cyber security in nearly 750,000 UK businesses lack the trained people[4] to carry out the kinds of basic tasks laid out in the national Cyber Essentials scheme[5] – then if paying attention to Employee Experience means we'll get more people to enter the profession, and stay in it, then pay attention to it we must.

Reference

1 Gartner Glossary. Available at: https://www.gartner.com/en/human-resources/glossary/employee-experience

2 Security Automation Market (2023). MarketsandMarket. Available at: https://www.marketsandmarkets.com/Market-Reports/security-automation-market-266165.html

3 Toon, C. (4 August 2023) UK's cyber security skills gap 'a ticking time bomb' for industry. Pinsent Masons. Available at: https://www.pinsentmasons.com/out-law/news/uks-cyber-security-skills-gap-a-ticking-time-bomb-for-industry

4 Coutinho, S., Bollen, A., Weil, C., Sheerin, C., Silvera, D., Donaldson, S., Rosborough, J. (2023) Cyber security skills in the UK labour market 2023 Findings report. Department for Science, Innovation & Technology. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1173325/

5 Cyber_security_skills_in_the_UK_labour_market_2023.pdf