"What Keeps People Secure is That They Met The Security Team": Deconstructing Drivers And Goals of Organizational Security Awareness

Jonas Hielscher (Ruhr University Bochum) and Simon Parkin (TU Delft)

The work was supported by the PhD School "SecHuman – Security for Humans in Cyberspace" by the federal state of NRW, Germany, and partly also by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

Security Awareness & Training (SAT)

SAT is big business

CISOs perceive SAT different from academic theory

Regulations might drive SAT growth

Security Awareness Training Market To Hit $10 Billion Annually By 2027

SACBT solutions are a major growth driver Download Report

– Steve Morgan, Editor-in-Chief

Sausalito, Calif. – Apr. 17, 2023

As the damage caused by cybercrime continues to escalate, industry leaders are bolstering their efforts to combat the threat. Consequently, the demand for security awareness training will continue rising. Cybersecurity Ventures predicts the global security awareness training market will exceed $10 billion annually by 2027, up from around $5.6 billion in 2023, based on 15 percent year-over-year growth.

https://cybersecurityventures.com/security-awareness-training-market-to-hit-10-billion-annually-by-2027/

Vista Equity Partners acquires KnowBe4 in $4.6bn deal

January 2023 | DEALFRONT | PRIVATE EQUITY & VENTURE CAPITAL

Financier Worldwide Magazine

January 2023 Issue

https://www.financierworldwide.com/vista-equity-partners-acquires-knowbe4-in-46bn-deal

"Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security

Jonas Hielscher and Uta Menges, *Ruhr University Bochum;* Simon Parkin, *TU Delft;* Annette Kluge and M. Angela Sasse, *Ruhr University Bochum*

https://www.usenix.org/conference/usenixsecurity23/presentation/hielscher

This paper is included in the Proceedings of the 32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Security Awareness Compliance Requirements

Like we said on our Getting Approved page, there are over 8,500 Local, State and Federal standards that your organization might need to comply with. Here is a list of the most common standards and regulations that may require your organizations to have a security awareness program in place. *Does your organization accept credit cards?* Well, in that case PCI-DSS is in force, and you need to train all staff about data security. (We have a course for that)

1. PCI DSS
§12.6 – Make all employees aware of the importance of cardholder information security.
• Educate employees (for example, through posters, letters, memos, meetings and promotions).
• Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures. Download the official PCI standard.

Is your company public? You need to have a program in place:

2. Sarbanes-Oxley (SOX)
§404(a).(a).(1) – The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C 78m or 78o(d)) to contain an internal control report which shall – state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting. If you are planning to go public in the future, start now with a security awareness training project.

Work in the health care sector? You need to have a program in place:

3. Health Insurance Portability & Accountability Act (HIPAA)
§164.308.(a).(5).(i) – Implement a security awareness and training program for all members of its workforce (including management).

And it goes on

4. ISO/IEC 27001 & 27002
employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

https://www.knowbe4.com/resources/security-awareness-compliance-requirements/

Security Awareness & Training (SAT)

SAT is big business

CISOs perceive SAT different from academic theory

Regulations might drive SAT growth

What are the incentives for implementing/ buying SAT?

Jonas Hielscher and Simon Parkin – "What Keeps People Secure is That They Met The Security Team": Deconstructing Drivers And Goals of Organizational Security Awareness – USENIX Security 2024

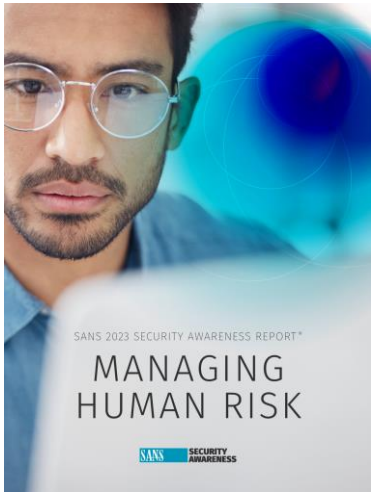
SAT Managers

- Dedicated SAT managers can only be found in larger organizations.
- Often, they have multiple roles, likes Information Security Officer + SAT Manager

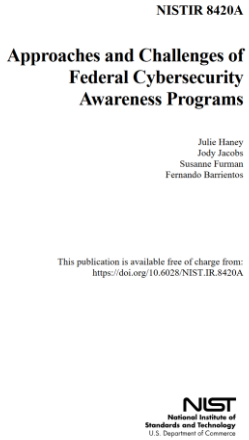
Jonas Hielscher and Simon Parkin – "What Keeps People Secure is That They Met The Security Team": Deconstructing Drivers And Goals of Organizational Security Awareness – USENIX Security 2024

SAT Managers

SANS Security Awareness Report
2023, 2022, 2021, …



Haney et al. (NIST)
SAT Managers in US Government


NISTIR 8420A

Approaches and Challenges of Federal Cybersecurity Awareness Programs

Julie Haney
Jody Jacobs
Susanne Furman
Fernando Barrientos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8420A

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Research Question

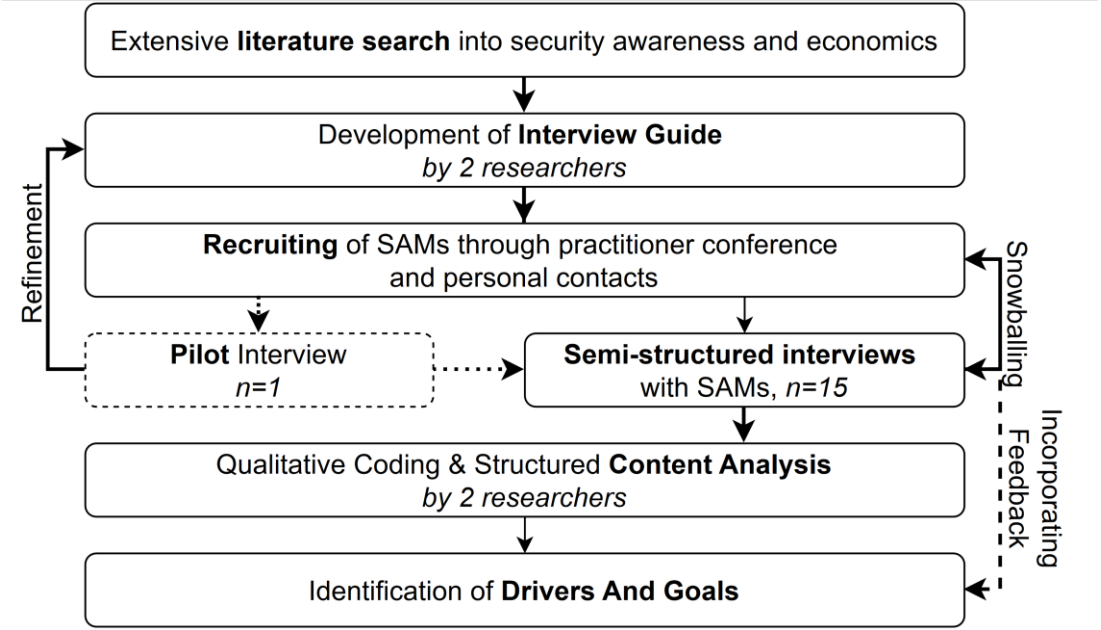
RQ1
What activities and topics do security awareness managers regard as being security awareness, within the remit of their role?

RQ2
How do security awareness managers interact with employees?

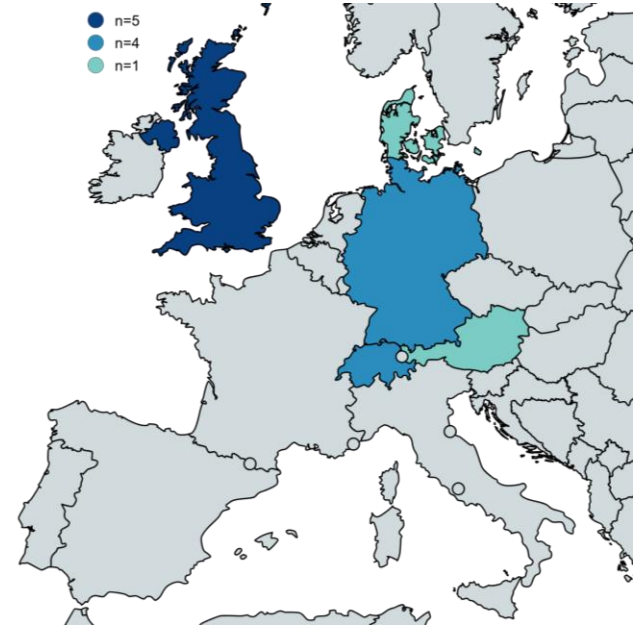
RQ3
How is success defined for security awareness managers, by them or others?

Method

- Semi-Structured Interviews with n=15+1 Full-Time Awareness Manager in Europe



Results



https://www.mapchart.net/europe.html

Table 1: Background information of the SAMs.

Gender	#	%	**Sector**	#	%
Female	10	*66*	Energy	3	*20*
Male	5	*33*	Consulting	3	*20*
Education			Banking	3	*20*
Cyber & Inf. Sec	5	*33*	Industry	2	*13*
CS & Engineering	4	*26*	Retail	2	*13*
Comm. & Marketing	2	*13*	Public	1	*6*
Social Science	2	*13*	Automotive	1	*6*
Education	1	*6*	**Country**		
Psychology	1	*6*	UK	5	*33*
Number of Employees			Germany	4	*26*
Max: 400,000 & *Min*: 1,600			Switzerland	4	*26*
Median: 27,000			Austria	1	*6*
Average: 62,000			Denmark	1	*6*

Results – Definition and Goal

- Completely distinct definitions
- Dislike the term “Security Awareness”
- Increased Security not main goal
- SAT might be self-serving

“When someone asks, ’Hey, do you do security awareness?’ and the person says, ’Yes.’ Then that can mean anything from, I wrote an email yesterday and next year I’m going to do this again, [...], to, I’m going to do it like company X [implementing a full security communication strategy]” – P3

“if more than 10 percent of people have actually read the article or reacted in some way, then it’s a success” – P1

“Sometimes there is a campaign that just doesn’t succeed. So we did spear phishing, we were too secure. So the emails didn’t get in, my people were already too aware. [...] we paid so much money [for the campaign].” – P4

Results - Activities

Phishing Simulations are the Nr. 1 SAT, followed by e-learning and active communication into the organization

Only few seek face-to-face contact

Organizations Security Policies shape SAT

Changing Threat Landscapes shape SAT

“Phishing, I try to minimize it where I can, but must, so a regulatory default actually with us, must be made” – P9

“What keeps people secure will absolutely not be the cybersecurity awareness training they had to do on onboarding. What it will be is the fact that during that onboarding they met the cybersecurity team or somebody from it, or they had an onboarding before they were even in the company they were maybe taken through” – P11

“At the moment there is a huge vishing campaign by some attackers, especially in our sector. And it’s happening relatively quickly. So the topic came to me, too, but it also popped out at [the CISO].” – P4

Results – Measurments

- Everyone measures SAT “success”
- Engagement > Knowledge
- ~~Behavior~~
- Struggles

“What are the access rates on the volunteer awareness blog? Yes, I measure that, how successful we are.” – P4

“We have already had many discussions about how to measure security awareness, whether we can somehow measure that people are aware of it. But somehow we haven’t found any good solutions yet.” – P1

“How click-through rates change, I think that’s what most people mention first. And where they also say, I’m measuring behavior like that, where I’m like, ’No, you’re not.’” – P9

Results – External Influences

- Vendors are brought in to compensate missing (human) resources
- Regulations heavily influence SAT, but the managers aim to hide this
- Regulations also create friction
- Disconnect between SAT managers and technical security teams

"We used to do that [content creation] ourselves, fortunately, we bought it from a vendor." – P2

"one of the biggest changes of the requirement for the new [regulation] is that you have to teach them. [...] why am I teaching somebody in a retail store, who has no access to the computer and only a pay machine, why am I teaching them about phishing? They don't even have an email address." – P10

"Just because it's written down doesn't make it true. [...] and of course, I'm just an aware ness person. So what do I know about these things?" – P10

Results – Employees

Some managers would like to reduce the questions they get from employees

Most would like to make SAT mandatory

Only in two cases would employees wishes inform SAT content

UK managers wanted to include usable security efforts

“Onboarding in particular is to be mandatory. The phishing simulations will soon be mandatory.” – P7

“At the same time, we try to train that e-mails should get encrypted. That works less well because, of course, that's something you have to do actively. But that's something we try to teach.” – P1

“We now try and understand why it's happening and what's happened [...] what comes out of it is things like there's a process that is broken and there's no other way to do it [...] and comms would never fix. So we work quite closely with security operations on that to try and find those human risks rather than, you know, just putting up comms.” – P15

Take Aways

SAT is underspecified and its goal is engagement and visibility rather than better security behavior.

- SAT is combination of tangible activities, material delivery and ongoing engagement for visibility. Academic research needs to look at SAT as a discipline of communication in practice.

SAT managers are in an employee-facing security-role, yet they are not responsible for usable security efforts. UK based managers would like to be in that role.

No one measures the “real success” of SAT. Engagement is used as a proxy for secure behavior.

Thanks!

"What Keeps People Secure is That They Met The Security Team": Deconstructing Drivers And Goals of Organizational Security Awareness

Jonas Hielscher
Human-Centred Security
Ruhr University Bochum, Germany

Simon Parkin
Cybersecurity (Technology, Policy, and Management)
Delft University of Technology, Netherlands

Abstract

Security awareness campaigns in organizations now collectively cost billions of dollars annually. There is increasing focus on ensuring certain security behaviors among employees. On the surface, this would imply a user-centered view of security in organizations. Despite this, the basis of what security awareness managers do and what decides this are unclear. We conducted $n = 15$ semi-structured interviews with full-time security awareness managers, with experience across various national and international companies in European countries, with thousands of employees. Through thematic analysis, we identify that success in awareness management is fragile while having the potential to improve; there are a range of restrictions, and mismatched drivers and goals for security awareness, affecting how it is structured, delivered, measured, and improved. We find that security awareness as a practice is underspecified, and split between messaging around secure behaviors and connecting to employees, with a lack of recognition for the measures that awareness managers regard as important. We discuss ways forward, including alternative indicators of success, and security usability advocacy for employees.

had anticipated [2]. This raises questions as to the incentive structure and mechanisms of change, that would drive adoption of improved practices as derived in prior research. It is then natural that in recent years, guiding employees to behave securely has grown to be a business function in its own right – worth billions [77]. A heavy focus of work in this space has been on designing effective interventions focusing on secure behavior, but less on how these interventions are effectively positioned within the specific setting of an organization.

Prior work has illustrated how drivers and goals, especially relating to security, may differ between employees [16] and the managers of the system. Research up to now has focused on what the apparatus allows an awareness campaign to achieve – where it has been questioned whether security awareness campaigns in organizations exist only to achieve security awareness [13]. Less attention has been given to the decisions and drivers that shape what is possible for a Security Awareness Manager (SAM) to achieve in their role [29], though there has been work exploring the requirements for e. g., US local government awareness campaigns to succeed [40]. This prompts a need to determine if secure working behavior is the only driver influencing the activities of a SAM, and in turn, security awareness programs.

jonas.hielscher@ruhr-uni-bochum.de or
S.E.Parkin@tudelft.nl

The work was supported by the PhD School "SecHuman – Security for Humans in Cyberspace" by the federal state of NRW, Germany, and partly also by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.