KnowBe4

Thought Leadership Series: Security Behavior Insights

Cybersecurity Information Sharing as an Element of Sustainable Security Culture

By Martin Kraemer

Good employee training heavily relies on three elements: content, experience, and relationships - the right content must be delivered through appropriate channels to the right people at the right time.

While employers strive to meet this challenge, the fact that employees already consume and share cybersecurity information at home and work is often overlooked. Consuming and sharing cybersecurity information is a desired behavior and an indicator of a good cybersecurity culture. Cybersecurity awareness and culture professionals know this. They appreciate the value of working with people to understand their existing security practices and empower them to improve their behavior.

Why, how, and what cybersecurity news people share

A strong security culture shows in proactive engagement with good security practices, mutual support and reassurance between employees, and a good understanding of the value and meaning of cybersecurity at an organization. A good culture also shows in people caring to share information. However, any cybersecurity culture is part of organizational culture which in turn is also influenced by social culture. The culture that surrounds us influences our ideas, values, and customs.

A key element of any cybersecurity strategy is effective communication with stakeholders. Effective communication is the foundation of any workplace training. To reduce human risk, we must win our workforce's hearts and minds to influence their behaviors. This feat starts with conveying information, turning it into knowledge, highlighting responsibilities, and influencing attitudes to increase motivation. All of these components together enable good security behaviors.

The relationship between proactive communication among the workforce and a good security culture is reflected in KnowBe4's security culture maturity model. Proactive sharing of cybersecurity-related information is a sign of a good security culture. Good security behaviors are the fabric of a healthy security culture that permeates private and professional life. A good security culture leads to more secure behaviors at home and at work, e.g., using password managers.

Security culture maturity can be measured

Employees at an organization with a good security culture are more likely to proactively engage in protecting the business, e.g., when spotting social engineering attacks or reporting cybersecurity incidents. At KnowBe4, we developed a security culture survey based on seven dimensions, and many of our customers use this survey to determine the maturity of the cybersecurity culture at their organization. According to the KnowBe4 2024 Security Culture Report, organizations in Europe perform slightly worse across most of these dimensions, i.e., attitudes, cognition, communication, compliance, and norms. However, they outperform the U.S. when it comes to the behavior dimension. Differences in security culture across organizations are measurable, and the better the security culture of an organization, the more protected the organization.

Facilitate cybersecurity information sharing

So long as cybersecurity challenges stay top of mind, employees are more likely to draw on their training when they need it (knowledge recall). Active and multi-faceted communication spreads knowledge, builds relationships, and increases the sense of belonging.

Our own Dr. Martin J. Kraemer (Security Awareness Advocate, Europe & the Middle East) teamed up with Dr. William Seymour (Assistant Professor in Cybersecurity of King's College London) to investigate how people consumed and shared cybersecurity news with friends, family, and work colleagues. They also aimed to understand the impact of workplace training across four major countries in the Global West, the U.S., the UK, Germany, and France.

The goal: understanding why, how, and what cybersecurity information people consume and share allows us to improve cybersecurity awareness and culture.

People (Want To) Care About Cybersecurity

An often-quoted truth about human nature is, "Just because I'm aware does not mean that I care". Knowledge of a threat is not the same as the desire to protect oneself, let alone is it the same as the intention to act. Security awareness professionals know this and hence focus on influencing behavior over delivering knowledge and information.

However, that does not mean people can change their behavior without reason. On the contrary, "knowing your why" is commonly associated with making positive changes to routines and habits. The same is true for security behavior. That is why effective communication to convey threats and dangers alongside advice and solutions is a key element of security culture.

Our survey results indicate that cybersecurity is a topic of conversation for many people. Cybersecurity has arrived in people's lives. People want to read, learn, and share relevant information to protect themselves and others. Almost all respondents (95%) had read or watched cybersecurity content at least once, and 77% had been at the receiving end of cybersecurity information sharing.

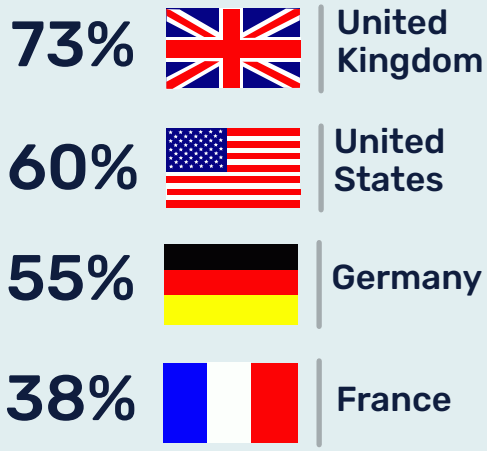
But what is it about cybersecurity that people find so intriguing?

The last cybersecurity news our respondents remembered fell into one of many categories, with data breaches (22%), phishing (17%), and hacking (15%) being the most popular among them. This is unsurprising. Data breaches and hacking frequently hit high-profile news headlines while phishing is something many banks or online shops warn their customers about, and it is also an important topic in corporate environments.

Where do people find cybersecurity information?

Security awareness is also the art of delivering the right knowledge, at the right time, to the right audience while using the right format. Security awareness professionals strive to maximize knowledge retention among their target audience. The source of cybersecurity news among our respondents was different depending on the age of

57% of people surveyed received cybersecurity-related training



Demographics

After cleaning up data from survey responses, the final dataset comprised 277 responses from France (average age 31), 238 from Germany (average age 32), 288 from the United Kingdom (average age 41), and 292 from the United States (average age 41). Most respondents were in full-time employment (56%), followed by part-time employment (18%), unemployed (7%) or not in paid work (7%), some were due to start a job within the next month (2%), and 9% stated other or undisclosed. Among the respondents from France and Germany, 52%, in the UK 63% and in the U.S. 67% were in full-time employment.

the respondent. While employers were generally an important source of cybersecurity information across all age groups, respondents frequently also used social media (age group 18–29), websites (age group 30-39 and 60-69), direct sharing (age group 40-49) and broadcasts and podcasts (age group 50-59) as additional sources of information. These differences in preference have an impact on what news people might find, as not all information is shared equally across all channels. More on that later.

Why do people share cybersecurity information?

People not only consumed information from various sources, but they also chose to share information on cybersecurity with others (25%). The act of sharing information with other employees is a desirable security behavior. It strongly suggests that people are aware and that they do care. They even want others to know and care about cybersecurity. Among our respondents who received cybersecurity news from others, no matter who shared the information, the assumption was that the spouse, family member, friend, or colleague wanted the respondent to protect themselves. The second most popular reason was to assume that the story was related to the sender's personal experience. The motivation to forward cybersecurity information was similar to what respondents expected others to care about when sharing information with them. Respondents wanted to protect themselves, help others protect themselves, or share a story relevant to their personal experience.

Key takeaway: Awareness is a key ingredient in shaping behavior

The more you care, the more you (want to) share

If we read more and learn more, we might also care more and share more. But without knowing the types of threats that exist, people cannot be aware of the need or even the possibility to change their behavior.

Our survey shows that respondents with higher security and privacy scores shared more cybersecurity information with partners, family, friends, and colleagues, showcasing why knowledge is important for fostering a security culture.

This is why it is important to answer the following questions:

- How can we provide the right content that people like, and we need them to see?
- How can we deliver this content in a manner that motivates consumption and sharing?
- How can we design content that helps to build relationships with the information security team and among people?

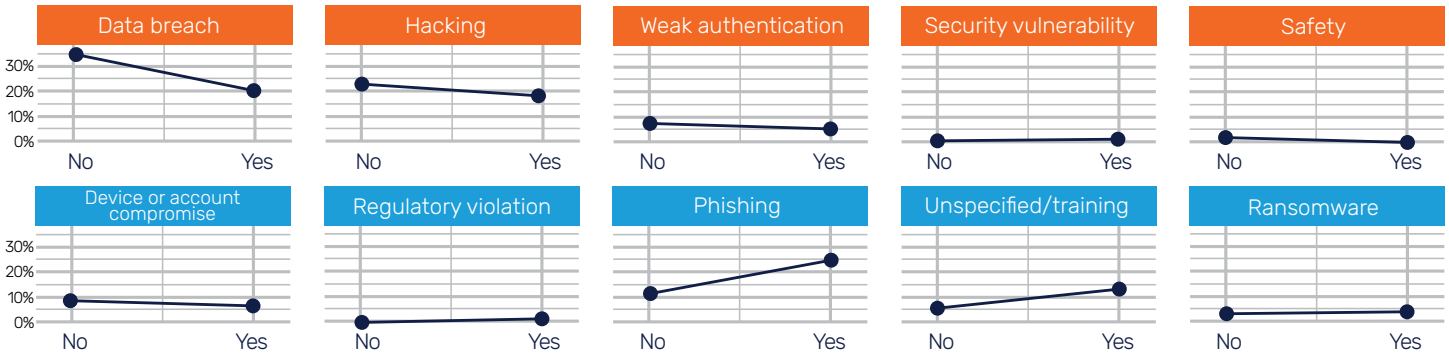
Where People Find Content and Why That Matters

Most respondents discovered cybersecurity content through websites (22%) and employers (21%), followed by social media (16%), direct sharing (15%), and broadcasts/podcasts (12%), with messaging from other companies (8%) and other means (5%) less common.

Respondents learned about different topics from different sources. The most common combination of source and topic were employers talking about phishing (7%), websites on data breaches (5%) and employers' delivery of unspecified 'awareness training' (5%), followed by someone private or a broadcasting station sharing information on data breaches (4%), and talk about hacking incidents on social media (4%).

The focus of workplace training on phishing over other content is notable. Those receiving workplace training were more likely to recall phishing-related content (+10.3%) and significantly less likely to mention data breaches (-10.1%). People who received training were also more likely to recall information from their training programs than from other sources.

Workplace training significantly affects the types of threats people recall reading or hearing about last



Receiving and Sharing Cybersecurity Information

Good training content offers actionable information. Respondents recognized that their organizations get this right, as employers were reported to be more likely to share 'solutions' than any other entity. Cybersecurity news, on the other hand, was more likely to be shared through broadcasts and podcasts.

Cybersecurity information from relationships and different media

Respondents most likely had cybersecurity information shared with them via message (45%), face-to-face (34%), social media (13%), calls (1%), or other means (7%). When respondents received cybersecurity news from others, it was most likely friends (32%) sharing news on data breaches (7%) or hacking incidents (7%). Note that 9% mentioned "hacking" as a topic that was shared on social media by 'others' whom they did not personally know.

When respondents received cybersecurity information from other people, the main topic of that information differed between different senders. Respondents received information from colleagues that was mainly on data breaches (5%) or phishing (4%). Respondents associated receiving information from friends with data breaches (7%), hacking (7%), or weak authentication (4%) rather than with other sources. This appears to be a deliberate choice, as organizations want their employees to be aware of data breaches and phishing in depth.

Key takeaway: Different cybersecurity topics are unequally distributed

Not all topics are covered equally by all sources

People have their preferences when it comes to discovering and consuming any information online, and it is known that certain platforms favor certain kinds of information, e.g., social media is known to host more polarizing information.[1]

The same is true for cybersecurity information that was discovered among our respondents. Not all topics were equally distributed across all sources, and there was a clear impact of workplace training on the type of information that people discovered and consumed.

Be mindful that employees not only consume cybersecurity information at work but also elsewhere. Professionals can use this reality to their advantage by either deliberately leading and influencing the conversation or by letting it develop freely.

- How do you know which cybersecurity issues your employees care about and what they know about them?
- Which topics are the most important for your organization?
- How do you address misconceptions and attitudes that are influenced by information sources outside work?

Note: We also recorded 5% of participants recalling workplace training as where they learned about cybersecurity last, but these participants could not remember the focus of training. Good training must be sticky and entertaining, and avoid training fatigue.

[1]Pew Research Center – News Platform Fact Sheet

People reportedly shared information which they found with others

Workplace training as received by the respondents in our sample did not motivate onward sharing. Respondents were also relatively less likely to share phishing information (-5.7%) and more likely to share ransomware news (6.7%) or generic information on a data breach (4.9%).

There are many potential reasons for that. Perhaps it was not possible to share information from workplace training with others due to technical limitations. Another possible explanation might be participants assuming that everyone else in the company will receive the same training and information. In any case, this is not a desirable outcome and should itself be addressed by training that encourages the sharing of cybersecurity information.

When prompted, people showed an appreciation for the benefits of sharing cybersecurity information with others. Respondents' propensity to share information was influenced by workplace training: respondents who received training were more likely to share with colleagues (23.6%). However, workplace training negatively impacted sharing intention with friends (-8.9%), family (-8.9%), and spouse (-5.3%).

Key takeaway: Enable and encourage cybersecurity information sharing across social circles

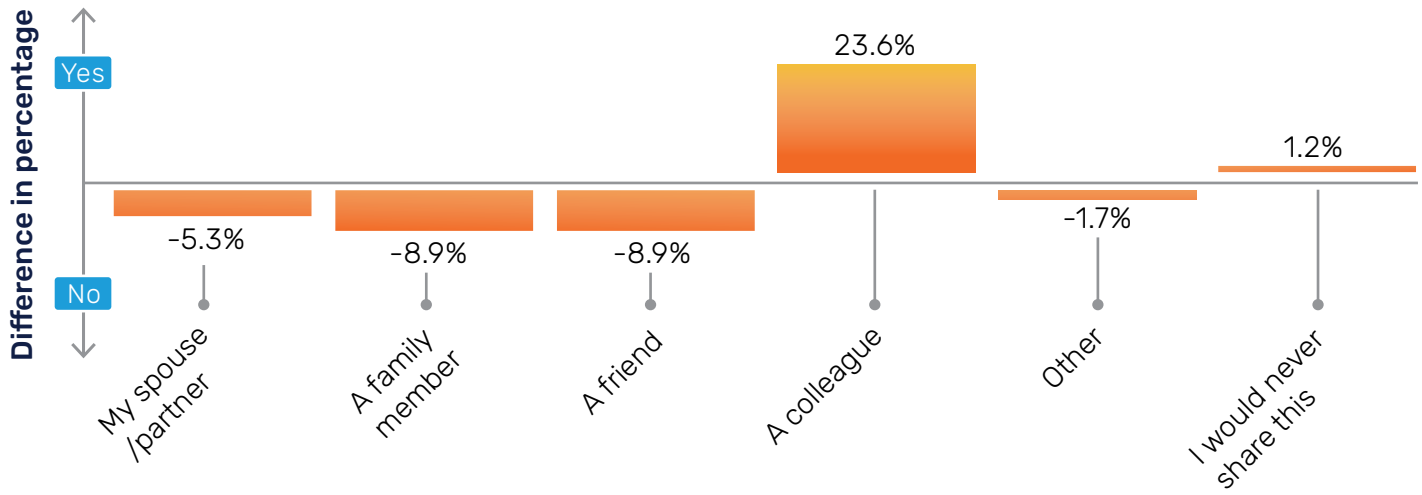
Remove sharing obstacles and empower people to cross social boundaries

Sharing cybersecurity information helps shape security culture. Training content should be shareable with all relevant social relationships, and training itself should encourage the sharing of information with relevant stakeholders.

- How can organizations cater to employees' sharing preferences to bridge the gap between work and home?
- How can organizations set incentives for the sharing of all relevant content?
- How should organizations prioritize topics and organize their training efforts across topics and communication media?

Organizations must explore these questions for their purposes as there is no one-size-fits-all answer.

Participants' inclination to further share cybersecurity information they received was also affected by whether they received workplace training



Recommendations

People care, and so should you
People care for each other and about cybersecurity. This is a fact that successful security awareness programs should leverage. Allow people to exercise care for their families, not just their colleagues. Perhaps, allow them to share access to particularly engaging content with their loved ones.

Back to basics
As obvious as it seems, a solid understanding of the foundations allows people to make better decisions according to expectations that are grounded in facts.

Deliver quality
The success of your program depends on the quality of your content. Workplace training affects what people recall regarding cybersecurity. Choose content that fits your goals deliberately.

Sit-in and take-away!
Make it easy to share cybersecurity information across personal and private life. There might be roadblocks that people face when they want to share information with their loved ones. Cybersecurity does not stop at the doorstep but affects people as much at home as at work.

Influencing cybersecurity information-sharing behavior
Provide the right content, in the right format, and with the right experience to motivate sharing. Facilitate sharing by opening communication channels for sharing.

Cultures are different
Keep in mind that individual and cultural differences impact the effectiveness of training, and design to reflect cultural differences. Ask the correct questions.

Cultural Influences Are Nuanced

Do not oversimplify cultural differences. While the country of residence might be a good indicator of preferred language and socio-political context, our findings also indicate that country of residence insufficient to explain cultural and contextual influences on attitudes and behaviors. Culture exists on the ground and has to be explored by professionals who design security programs.

Cybersecurity is a multifaceted issue that is appreciated differently by different people. That means security programs must cater to other personality types, learning styles, attitudes, and preferences. These individual differences are also reflected in larger cultural differences. However, we found country of residence to be a poor indicator for differences in content consumption and sharing behavior. All four countries in this study have multifaceted cultural communities with their own security attitudes, behaviors, media landscapes, languages, and the adoption of news channels. Anecdotally, we know that there are stark differences between preferences across countries.

Do not use countries as shorthand for discovering the culture on the ground. It is essential to familiarize yourself with the social behaviors, customs, and values that are the environment for security behavior. It is important to understand which culture you have before you can shape it. Get out there and learn through interviewing, surveying, and observing.

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk. For more information, please visit www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com