I. Introduction

The document "CYBSAFE-Oh, Behave! 2023-FINAL REPORT" is the 2023 Annual Cybersecurity Attitudes and Behaviors Report, which provides a comprehensive analysis of the current state of cybersecurity awareness, attitudes, and behaviors among internet users. It is structured to cover various aspects of cybersecurity, including people's online presence, their attitudes towards online security, the role of behavioral science in cybersecurity, and the effectiveness of cybersecurity training.

The complex relationship between human behavior and cyber security risks will be explored below, offering a unique perspective on the digital security landscape. The analysis will highlight key findings on improving the effectiveness of the organization's security methods, and will also serve as an essential resource for understanding and managing human cyber risks in an ever-changing threat landscape.

II. Executive Summary

It provides an overview of the current state of cybersecurity attitudes and behaviors across the United States, Canada, the United Kingdom, Germany, France, and New Zealand.

The key findings are:

- **Online presence**: Almost half (47%) of the participants have ten or more sensitive online accounts, like payment-related and primary email accounts. 15% admitted they'd lost count.
- **We're frustrated and doubtful about online security**: While 84% consider staying secure a priority, and 69% perceive it as achievable, a sizable 39% of participants felt frustrated, and 37% were intimidated by staying secure online. One in three (32%) often feel overwhelmed by cybersecurity information.
- **Move over cybersecurity training, nudges are coming**: Just over a quarter of participants (26%) reported having access to, and taking advantage of, cybersecurity training. Meanwhile, two-thirds (64%) noted they had no access to training whatsoever.
- **Are we behaving?**: The report investigates five key security behaviors: password hygiene, using Multi-Factor Authentication (MFA), installing the latest device updates, checking emails for signs of phishing and reporting them, and backing up data. However, the executive summary does not provide specific findings on these behaviors

A. *Online presence*

It outlines the following key points:

- **Daily Internet Use**: A significant 93% are being online at least once daily, with only 7% connecting less frequently
- **Sensitive Online Accounts**: Nearly half (47%) of the respondents have ten or more sensitive online accounts, which include those related to payments and primary email accounts
- **Lost Count**: A notable 15% of participants have lost count of how many sensitive online accounts they possess
- **Generational Differences**: Younger generations, such as Gen Z, reported having over 20 sensitive online accounts, indicating a larger digital footprint compared to older generations like Baby Boomers and the Silent Generation

B. *We're frustrated and doubtful about online security*

It provides several key findings and takeaways that underscore the need for more personalized and hands-on approaches to cybersecurity, as well as the importance of making security decisions and actions simpler and more manageable for individuals:

- **Security Fatigue**: Many people feel overwhelmed by the complexity of online security, leading to a sense of resignation and loss of control. Over half of the sample felt it was pointless to protect themselves, indicating a high level of security fatigue.
- **Need for Simplified Security Decisions**: limiting the number of security decisions people have to make, simplifying protective cybersecurity actions, and ensuring advice is consistent and doesn't introduce unnecessary friction to people's work.
- **Cognitive Miser Tendency**: People tend to rely on simple rules to make decisions due to limited cognitive resources such as time, knowledge, attention, and memory. This human tendency is referred to as being a 'cognitive miser'.
- **Security vs. Productivity**: The report highlights the delicate balance between the perceived benefits and

costs of engaging with security for individuals and businesses.

- **Frustration and Doubt**: A significant portion of participants felt frustrated (39%) and intimidated (37%) by staying secure online. One in three (32%) often feel overwhelmed by cybersecurity information, scaling down their online actions as a result.
- **Cost of Protective Action**: Almost half of the participants (49%) felt that taking protective action online comes at a high cost. While 69% thought staying secure online is worth the effort, younger generations were more skeptical about the return on investment.
- **Media Influence**: Over half of the participants (56%) said the news motivates them to take protective security actions, and 51% find the media/news coverage helps them stay informed about online security. However, 44% of the participants said the media evokes fear, and 42% felt it overcomplicates online security

C. *Move over cybersecurity training, nudges are coming*

It presents several key points and findings that suggest a need for more accessible cybersecurity training, especially for non-working individuals. The shift towards security alerts indicates a preference for proactive, real-time security measures. That there is an opportunity to improve cybersecurity awareness and practices through better dissemination of available resources and the implementation of more engaging, user-friendly security strategies

- **Cybersecurity Training Access**: only about a quarter (26%) of participants have access to and take advantage of cybersecurity training. A significant majority (64%) reported having no access to such training at all.
- **Online Cybersecurity Training Preference**: a preference for online cybersecurity training. Participants who had completed courses found the content useful and engaging, whether they were learning at home or in work environments.
- **Shift Towards Security Alerts**: There is a noticeable shift towards different strategies to engage with security. More people are opting for timely notifications or alerts when making decisions that could put them at risk.
- **Vulnerability of Non-Working Individuals**: Retired individuals or those not in active employment remain vulnerable as they report little to no access to training resources.

1) *Main Argument of "Move Over Cybersecurity Training, Nudges Are Coming"*

The main argument is that while traditional cybersecurity training is beneficial, there is a significant portion of the population that does not have access to such training. Only 26% of participants reported having access to and taking advantage of cybersecurity training, leaving a vast majority without the resources to learn about cybersecurity best practices.

It is useful to do a shift in how people engage with security, with an increasing preference for timely notifications or alerts when making decisions that could put them at risk. This indicates a move towards more proactive and context-aware methods of cybersecurity education, such as nudges, which can provide just-in-time guidance and reminders to users.

It highlights the vulnerability of certain groups, such as retirees and those not in active employment or studying, who report little to no access to training resources. This suggests a need for better publicity of high-quality, free cybersecurity content available on the internet to these audiences.

In essence, it argues for a broader and more inclusive approach to cybersecurity awareness that goes beyond traditional training and incorporates behavioral strategies to engage users in security practices effectively.

2) *Nudges in cybersecurity*

Nudges in cybersecurity differ from traditional cybersecurity training in several ways. Traditional cybersecurity training often involves formal sessions where users are taught about various threats and how to protect against them. This training can be time-consuming and often requires users to remember a lot of information. On the other hand, nudges are subtle prompts or suggestions designed to influence behavior in a predictable way, without restricting any options or significantly changing economic incentives. They are often integrated into the systems that users interact with daily, making them less intrusive and more contextually relevant.

Nudges can be used to encourage better cybersecurity practices in various ways. For example, nudges can be used to prompt users to create longer and more secure passwords, reducing the likelihood of account breaches. They can also be used to encourage the use of multi-factor authentication (MFA), further enhancing account security. Nudges can also be used to encourage users to regularly update their software, protecting them from vulnerabilities that cybercriminals could exploit.

3) *Addressing Security Fatigue with Nudges*

To address security fatigue when using nudges to improve cybersecurity, it's essential to:

- **Limit Security Decisions**: Reduce the number of security decisions users must make, such as by implementing Single Sign-On (SSO) to avoid multiple password prompts
- **Simplify Protective Actions**: Make it easy for users to take protective cybersecurity actions, ensuring that the process is straightforward and user-friendly
- **Consistent Advice**: Provide consistent and clear advice that doesn't introduce confusion or unnecessary friction, which can contribute to security fatigue

4) *Personalized and Hands-On Cybersecurity Awareness Activities*

Examples of personalized and hands-on approaches to cybersecurity awareness activities include:

- **Interactive Training**: Engage users with interactive training sessions that simulate real-world scenarios, such as phishing simulations or cybersecurity escape rooms

- **Gamification**: Use games and challenges to make learning about cybersecurity fun and engaging, such as cybersecurity-themed crossword puzzles or capture-the-flag competitions
- **Storytelling and Skits**: Tell stories or perform skits that illustrate cybersecurity concepts in an entertaining and relatable way
- **Small-Group Activities**: Conduct small-group activities that encourage discussion and hands-on practice of cybersecurity principles
- **Incentivization**: Offer unconventional prizes or incentives to motivate participation in cybersecurity awareness activities

5) Nudges Benefits

There are several potential benefits of using nudges to improve cybersecurity.

Firstly, nudges can help to reduce security fatigue, a state of weariness or reluctance to deal with cybersecurity issues, by simplifying and integrating security decisions into users' daily routines. This can make security practices more manageable and less overwhelming for users.

Secondly, nudges can help to balance security and productivity. Traditional cybersecurity measures can often hinder users' primary tasks, making them less likely to follow security practices. By integrating security decisions into users' workflows, nudges can help to ensure that security practices do not interfere with productivity.

Thirdly, nudges can help to overcome generational challenges in cybersecurity. Different generations may have different attitudes and behaviors towards cybersecurity, and nudges can be tailored to meet the specific needs and preferences of different user groups.

Nudges can help to foster a culture of security within organizations. By encouraging users to take small, manageable steps towards better security practices, nudges can help to create an environment where security is seen as a shared responsibility and a normal part of daily activities.

6) Nudges Drawbacks

While nudges can be a useful tool in improving cybersecurity, they must be carefully designed and implemented to avoid these potential drawbacks. They should be part of a broader cybersecurity strategy that includes technical measures, education, and a culture of security.

There are several potential drawbacks to this approach:

- **Security Fatigue**: Constant decisions about online security can lead to 'security fatigue', where people become desensitized to the dangers of the internet. This can result in feelings of helplessness and resignation, making it harder to motivate individuals to take protective actions
- **Cognitive Load**: People tend to rely on simple rules to make decisions due to limited cognitive resources such as time, knowledge, attention, and memory. If the number of security decisions is too high, it can overwhelm individuals and lead to poor decision-making
- **Security vs. Productivity**: There is often a delicate balance between the perceived benefits of security measures and their costs to individuals and businesses. If security measures hinder people's primary goals, they are less likely to take protective cybersecurity measures. This can be seen in behaviors such as backing up data, using multi-factor authentication (MFA), and managing passwords
- **Trust Issues**: There can be a lack of trust in certain security tools, such as password managers. Despite being considered the safest option, many people still have reservations about using them due to concerns about their security and the potential for all their passwords to be compromised at once
- **Lack of Reporting**: Many people do not report phishing attempts, either because they don't know how, can't find the reporting buttons, or believe that reporting won't stop cybercriminals. This lack of reporting can allow phishing attempts to continue unabated
- **Generational Challenges**: Different generations have varying levels of confidence and ability in recognizing and dealing with cybersecurity threats. For example, older generations are generally less confident in their ability to recognize phishing messages
- **Ineffectiveness of Awareness & Education**: Simply being aware of the risks and knowing how to install updates or recognize phishing attempts does not always lead to the right behaviors. Many people still procrastinate or ignore updates, and some do not check messages for signs of phishing before taking action

7) Balancing Perceived Benefits and Costs with Nudges

To balance the perceived benefits and costs of cybersecurity when using nudges:

- **Highlight Immediate Benefits**: Emphasize the immediate benefits of secure behavior, such as the peace of mind that comes from knowing one's data is protected
- **Minimize Perceived Costs**: Design nudges that minimize the perceived costs of security measures, such as using auto-updates to reduce the effort required from users
- **Cultural Relevance**: Ensure that nudges are culturally relevant and resonate with the target audience, which can increase their perceived value
- **Feedback and Recognition**: Provide feedback and recognition for secure behaviors, reinforcing the benefits and encouraging continued compliance

D. Cybercrime victims are reporting more

It outlines the following key points that highlight the importance of reporting mechanisms in the fight against cybercrime and the need for continued efforts to make reporting processes more accessible and effective. They also underscore the growing concern among internet users about the risk of becoming cybercrime victims.

- **Increase in Reporting**: A significant number of cybercrime victims are reporting incidents. The report indicates that 88% of participants who experienced cybercrime reported it to someone
- **Reporting by Crime Type**: Reporting rates varied by the type of cybercrime. For phishing, 59% reported to their bank or credit card company, while 54% of identity theft and 42% of online dating scam victims did the same
- **Prevention and Recovery Motivations**: The primary reasons for reporting cybercrimes like phishing, online dating scams, and identity theft were to prevent the crime from happening again to themselves or others, and to recover lost money
- **Challenges in Reporting**: While many knew how to report phishing scams (49%), some found the reporting process challenging. A quarter of identity theft victims found it difficult but eventually succeeded in reporting the crime
- **Reasons for Not Reporting**: Some victims chose not to report cybercrimes because they considered the loss negligible or believed that reporting would not lead to any action
- **Perception of Risk**: There has been a 7% increase in the number of people who feel they may become victims of cybercrime, with 50% of participants considering themselves potential targets

1) Reasons why cybercrime victims report incidents

The main reasons why cybercrime victims report incidents are to prevent the crime from happening again to themselves or others and to recover lost money. Specifically, for crimes like phishing, online dating scams, and identity theft, victims reported to prevent recurrence and to attempt to recover financial losses.

The top cited reasons for not reporting cybercrime incidents include a belief that reporting does not stop cybercriminals, with 72% of participants holding this belief. Other reasons include the desire to stop spam messages from getting into their inbox, a wish for something to happen when reporting them (such as receiving an acknowledgment), and a need for more trust in the reporting process.

The reporting of cybercrime incidents has changed over time, with an overall increase in reporting rates. For North American and British participants, phishing reporting rates were up by 19 percent on average from the previous year. Reporting rates for online dating scams increased by 45 percent for Canadian and British participants and by 19 percent for Americans. Identity theft reporting increased by 29 percent for British participants, 19 percent for Americans, and 11 percent for Canadians

2) Common Misconceptions About Reporting Cybercrime Incidents

Some common misconceptions about reporting cybercrime incidents include:

- **Reporting Leads to Publicity**: There's a belief that reporting cyber attacks to authorities will make the incident public, which can deter organizations from reporting due to fear of reputation damage
- **Paying Ransom Solves the Problem**: Another misconception is that paying a ransom will automatically resolve the incident, which is not always the case and can perpetuate the cycle of crime
- **Reporting is Futile**: Many think that reporting does not stop cybercriminals, which can lead to underreporting. This belief is held by 72% of participants in the CYBSAFE report
- **Reporting is Too Complex**: The process of reporting can be seen as too complex or time-consuming, which can discourage victims from coming forward
- **Fear of Consequences**: There's a fear that reporting might lead to legal trouble or unwanted scrutiny, which can prevent organizations from reporting incidents

3) Encouraging Employees to Report Cybercrime Incidents

Organizations can encourage employees to report cybercrime incidents by:

- **Creating a Supportive Culture**: Fostering a blame-free culture where employees feel comfortable reporting incidents without fear of repercussions
- **Providing Training and Awareness**: Regularly training employees on the importance of reporting and how to do it effectively
- **Implementing Reporting Mechanisms**: Making the reporting process simple and accessible, possibly with anonymous options as a last resort
- **Demonstrating Action**: Showing that reports lead to action and improvements can motivate employees to report
- **Communicating the Importance**: Explaining to employees how reporting helps the organization and protects everyone's interests

4) Potential Consequences of Not Reporting Cybercrime Incidents

The potential consequences of not reporting cybercrime incidents include:

- **Financial Loss**: Organizations may suffer financial losses due to fraud, theft, or ransom payments
- **Reputation Damage**: Even if incidents are not reported, they can become public and damage the organization's reputation
- **Operational Downtime**: Not reporting can lead to prolonged operational downtime as the organization struggles to recover from the incident
- **Legal and Regulatory** Consequences: Failure to report can result in legal claims, regulatory fines, and non-compliance with data protection laws
- **Erosion of Trust**: Customers and partners may lose trust in an organization that fails to manage and report cybercrime effectively

E. Are we behaving?

It provides key insights into the cybersecurity behaviors and attitudes of individuals. These findings highlight the importance of cybersecurity awareness and training, the influence of media on cybersecurity perceptions, and the need for effective reporting mechanisms for cybercrime incidents.

- **Online Presence**: almost half (47%) of the participants have ten or more sensitive online accounts, such as payment-related and primary email accounts. Additionally, 15% admitted they'd lost count
- **Media Influence**: Over half of the participants (56%) said the news motivates them to take protective security actions, and 51% find the media/news coverage helps them stay informed about online security. However, 44% of the participants said the media evokes fear, and 42% felt it overcomplicates online security
- **Access to Training**: Just over a quarter of participants (26%) reported having access to, and taking advantage of, cybersecurity training. Meanwhile, two-thirds (64%) noted they had no access to training whatsoever
- **Cybercrime Reporting**: Most participants (88%) reported their cybercrime experiences to someone. Incident reporting rates were favorable for all crime types. Only a small percentage of incidents which led to data or money loss went unreported: 14% of phishing, 16% of online dating scams, and 8% of identity thefts

III. THE MAIN FINDINGS

These findings underscore the importance of understanding and addressing the human factors that contribute to security breaches and incidents. They also highlight the need for effective cybersecurity training and the role of media in shaping perceptions and behaviors related to online security.

A. Cybersecurity Behaviors and Practices

- **Software Updates**: Despite the importance of software updates in protecting against cyber threats, many individuals and organizations procrastinate or ignore them. This behavior can lead to significant vulnerabilities, as seen in the WannaCry ransomware attacks
- **Phishing Awareness**: While 65% of participants claimed they knew how to install the latest software and application updates, 18% admitted the opposite, and another 17% knew how but tended not to install the updates. This shows that awareness and education do not always lead to the right behaviors
- **Phishing Reporting**: Only 44% of participants reported making use of 'spam' or 'report phishing' buttons 'very often' or 'always'. A significant 33% of participants are not taking action against cybercriminals
- **Password Hygiene**: Many people prefer their own methods of password management, such as writing them down in notebooks. They do not trust having all their passwords sit within one tool, especially given the recent media attention on password managers failing to protect users

B. Cybersecurity Responsibility

- **Generational Differences**: Gen Z and Millennials tend to have a "laissez-faire" attitude towards online security. They don't prioritize online security as much as older generations, and half didn't think staying safe online was worth their effort. Cybercrime among these generations was noticeably higher than other generations
- **Role of Media**: Media coverage can increase motivation to take action to protect oneself. However, it can also lead to people miscalculating risks, simply because it has been in the news recently (i.e., availability bias)
- **Cybersecurity Training**: Access to cybersecurity training is not universal. Retired individuals or those not in active employment report little to no access to training resources. Online cybersecurity training was preferred overall, and those who had completed courses found training content useful and engaging

C. Generational Differences in Attitudes Towards Online Security

- **Gen Z and Millennials**: These generations tend to have a more relaxed attitude towards online security. They don't prioritize it as much as older generations, and half didn't think staying safe online was worth their effort. Cybercrime among these generations was noticeably higher than other generations
- **Older Generations**: Older generations were overall less confident in their ability to recognize phishing emails. For example, 20% of the Silent Generation and 17% of Baby Boomers expressed doubt in their ability to recognize phishing messages

D. Cybercrime Victimization

These findings highlight the varying levels of cybercrime victimization across different countries and the types of cybercrimes that are most prevalent.

- **Global Outlook on Cybercrime Victimization**: Attitudes towards the likelihood of becoming a victim of cybercrime were indifferent globally. However, Germans (45%) felt the least worried about falling victim to cybercrime compared to other countries, which ranged from 57% to 63%
- **Cybercrime Victimization by Country**: Americans (61%) had a reason to be worried about becoming a victim of cybercrime, as over a third (36%) of them reported having been a victim of one or more cybercrime types. Canadians (23%) and Germans (23%) had the lowest cybercrime victim numbers
- **Type of Cybercrime**: Americans were consistently more likely to have been a victim of any type of cybercrime. When examining each crime type, Americans (27%) reported most of the identity thefts compared to other countries - especially participants from France (9%). Compared to other cybercrimes, British participants (19%) were more likely to fall victim to online dating scams than other crime types (16% phishing and 18% identity theft)

IV. Attitudes towards Online Security

These findings highlight a positive attitude towards online security among most participants, but also reveal significant challenges, such as frustration, intimidation, and the feeling of being overwhelmed by cybersecurity information. The data also shows a generational divide in attitudes towards the value of online security efforts and the impact of media on public perception.

- **Priority and Achievability**: A strong majority of participants, 84%, consider staying secure online a priority, and 69% believe it is achievable
- **Frustration and Intimidation**: Despite the importance placed on security, 39% of participants felt frustrated and 37% felt intimidated by the process of staying secure online
- **Overwhelmed by Information**: One in three (32%) participants often feel overwhelmed by cybersecurity information, which leads them to scale down their online actions
- **Cost of Security**: Almost half of the participants (49%) perceive that taking protective action online comes at a high cost. However, 69% still think staying secure online is worth the effort
- **Generational Skepticism**: Younger generations, specifically 21% of Gen Z and 23% of Millennials, are more than twice as likely as Baby Boomers (6%) and the Silent Generation (9%) to doubt whether the effort to stay secure online is worth it
- **Media Influence**: Over half of the participants (56%) said the news motivates them to take protective security actions, and 51% find media/news coverage helps them stay informed about online security. However, 44% said the media evokes fear, and 42% felt it overcomplicates online security

V. Cybersecurity Training

These findings underscore the importance of cybersecurity training in the workplace and highlight the varying approaches to cybersecurity education across different countries. The data also suggests that making cybersecurity training mandatory could potentially increase its uptake, as seen in the case of the UK.

- **Access to Cybersecurity Training**: half of the participants from Canada (59%), New Zealand (57%), the UK (56%), and Germany (51%) accessed cybersecurity training at their workplaces. A third of participants from the US (33%) and Germany (33%) reported accessing training at home, while French participants (23%) were more likely to access training in a public location, such as a library
- **Mandatory Training**: the completion of mandatory cybersecurity training at work or a place of education was highest among British participants (88%) and lowest among French participants, with almost a quarter (24%) reporting cybersecurity training as a non-mandatory exercise
- **Total Number of Participants**: The study was conducted among 6064 participants from the US, Canada, UK, Germany, France, and New Zealand. Out of these, 2065 participants had access to cybersecurity training

VI. Conclusion

In conclusion it summarizes several key findings as follows:

- **Security Fatigue is Real**: many people feel overwhelmed by the amount of cybersecurity information, which can lead to reduced online activity. Almost half of the participants (49%) believe that taking protective action online is costly.
- **Security vs. Productivity**: conflict between maintaining security and productivity. While 69% of participants believe that staying secure online is worth the effort, younger generations (21% of Gen Z and 23% of Millennials) are more skeptical about the return on investment.
- **Generational Challenges**: generational differences in attitudes towards online security. Younger generations are more likely than Baby Boomers and the Silent Generation to doubt that online security is worth the effort.
- **The Role of the Media**: Over half of the participants (56%) said the news motivates them to take protective security actions, and 51% find the media/news coverage helps them stay informed about online security. However, 44% of the participants said the media evokes fear, and 42% felt it overcomplicates online security.
- **Cybersecurity Training**: importance of cybersecurity training, but does not provide specific findings or numbers in the conclusion section.

A. *Extended conclusions:*

- **Security Fatigue**: Many people feel overwhelmed by cybersecurity information, leading to reduced online activity and a perception that taking protective actions is costly.
- **Security vs. Productivity**: Younger generations are more skeptical about the return on investment for cybersecurity measures, balancing security with productivity.
- **Generational Differences**: Attitudes towards online security vary across generations, with younger generations expressing more skepticism and doubt about the value of cybersecurity efforts.
- **Media Influence**: The media plays a significant role in shaping perceptions of online security. While it can motivate people to take protective actions, it can also evoke fear and overcomplicate the issue.
- **Cybersecurity Training**: Access to cybersecurity training remains limited, with only a quarter of participants reporting access to training. However, those who received training reported positive changes in their cybersecurity behaviors.

- **Cybercrime Reporting**: Cybercrime reporting rates have increased, with most victims reporting incidents to relevant authorities. However, a significant number of incidents still go unreported due to perceived insignificance or lack of faith in authorities.
- **Cybersecurity Behaviors**: Password hygiene, MFA usage, device updates, phishing awareness, and data backup are key cybersecurity behaviors that need improvement.
- **Online Presence**: People have an extensive online presence, with many having ten or more sensitive online accounts. This highlights the need for robust cybersecurity practices.
- **Attitudes Towards Online Security**: While most people consider staying secure online a priority, many feel frustrated and intimidated by the process.
- **Cybersecurity Responsibility**: There is a need to foster a sense of shared responsibility for cybersecurity among individuals, organizations, and governments.
- **Nudges**: Nudges can be an effective tool to encourage positive cybersecurity behaviors, but they need to be personalized, hands-on, and address the perceived benefits and costs of cybersecurity measures.
- **Security Fatigue**: Security fatigue can be addressed by providing personalized and hands-on cybersecurity awareness activities that focus on the benefits of cybersecurity and address the perceived costs.
- **Cybersecurity Training**: Cybersecurity training should be accessible, engaging, and tailored to different audiences. It should also address the perceived benefits and costs of cybersecurity measures.
- **Cybercrime Reporting**: Encouraging cybercrime reporting requires addressing the reasons for non-reporting, such as perceived insignificance of incidents and lack of faith in authorities.
- **Cybersecurity Behaviors**: Improving cybersecurity behaviors requires addressing the perceived benefits and costs of cybersecurity measures, providing personalized and hands-on awareness activities, and balancing security with productivity.
- **Online Presence**: Managing an extensive online presence requires strong cybersecurity practices, including password hygiene, MFA usage, device updates, phishing awareness, and data backup.
- **Attitudes** Towards Online Security: Addressing negative attitudes towards online security requires addressing the perceived costs and benefits of cybersecurity measures, providing personalized and hands-on awareness activities, and fostering a sense of shared responsibility.
- **Cybersecurity Responsibility**: Fostering a sense of shared responsibility for cybersecurity requires addressing the perceived costs and benefits of cybersecurity measures, providing personalized and hands-on awareness activities, and addressing the perceived costs and benefits of cybersecurity measures.

B. Security Fatigue is Real

These findings underscore the reality of security fatigue among users, highlighting the need for more user-friendly and cost-effective cybersecurity measures, as well as clear and actionable information about online security.

- **Frustration and Intimidation**: A significant number of participants expressed frustration and intimidation about staying secure online. Specifically, 39% of participants felt frustrated, and 37% were intimidated by online security
- **Overwhelmed by Information**: One in three participants (32%) often felt overwhelmed by cybersecurity information, which led them to scale down their online actions
- **Cost of Security**: Almost half of the participants (49%) felt that taking protective action online was costly
- **Doubts about Effort Worth**: While 69% of participants thought staying secure online was worth the effort, younger generations (21% of Gen Z and 23% of Millennials) were more skeptical about the return on investment. They were more than twice as likely as Baby Boomers (6%) and the Silent Generation (9%) to doubt that online security is worth the effort
- **Media Influence**: Over half of the participants (56%) said the news motivates them to take protective security actions, and 51% find the media/news coverage helps them stay informed about online security. However, 44% of the participants said the media evokes fear, and 42% felt it overcomplicates online security

C. Security vs. Productivity

Key findings are as follows:

- **Balancing Act**: The report discusses the challenge of balancing security measures with productivity, acknowledging that overly complex or time-consuming security practices can hinder work efficiency and user compliance.
- **User Experience**: It may highlight the importance of designing security measures that are user-friendly and do not disrupt users' primary tasks, to ensure that security practices are adopted and maintained.
- **Behavioral Insights**: The subsection might also emphasize the use of behavioral insights to create security solutions that are not only effective but also align with users' work habits and preferences.
- **Productivity Concerns**: There could be a discussion on how productivity concerns can sometimes lead to poor security practices, such as using weak passwords for the sake of convenience, and how to address these concerns.
- **Security Integration**: The report may suggest ways to integrate security seamlessly into daily workflows, so that it enhances rather than detracts from productivity.

D. Generational Challenges

These findings indicate that there are significant generational differences in attitudes towards online security, with younger generations feeling less in control and more overwhelmed by cybersecurity information. This suggests a need for tailored cybersecurity education and communication strategies that resonate with different age groups

- **Generational Prioritization**: Older generations prioritize online security more than younger generations. For example, 91% of Baby Boomers consider staying secure online a priority compared to 69% of Gen Z.
- **Intimidation by Online Security**: The Silent Generation (43%) and Millennials (40%) experience the highest levels of intimidation by online security, while Gen X feels the least intimidated.
- **Skepticism About Effort**: Younger generations, specifically 21% of Gen Z and 23% of Millennials, are more than twice as likely as Baby Boomers (6%) and the Silent Generation (9%) to doubt that online security is worth their efforts.
- **Achievability of Online Security**: While 59% of Gen Z believe staying secure online is achievable, other generations agree at higher rates, ranging from 68% to 79%.
- **Feeling in Control**: Less than half of Gen Z (44%) feel in control of their online security, which is lower than the confidence expressed by other generations.
- **Overwhelmed by Information**: Younger generations, particularly Gen Z (35%) and Millennials (38%), and the Silent Generation (45%) feel overwhelmed by online security information and tend to minimize their online actions more than Gen X (29%) and Baby Boomers (28%)

E. The Role of the Media

These findings highlight the importance of the media in promoting online security awareness and the need for more accessible cybersecurity training.

- The media plays a significant role in shaping people's views towards online security. 59% of Germans agreed that media/news help them stay informed about online security, compared to 44% of New Zealanders and 47% of French participants
- The media also motivates people to take protective actions for their online security. 61% of Germans and Americans felt inspired to take protective action as a result of media/news coverage. However, New Zealanders felt least motivated by news/media coverage, with 48% agreeing and 14% disagreeing with the statement
- Despite the positive influence, 44% of the participants said the media evokes fear, and 42% felt it overcomplicates online security
- Overall, access to cybersecurity training was poor across the countries. 70% of French participants reported having no access to training, followed by Canadians (67%). Americans (44%) reported having the most opportunities to access cybersecurity training

F. Cybersecurity Training

These findings highlight the importance of cybersecurity training and its impact on improving security behaviors. They also suggest that while access to training is available to some, there is still a significant portion of the population that lacks access, indicating a need for broader availability and engagement in cybersecurity education initiatives

- **Access to Cybersecurity Training**: Over half of Canadians (59%), New Zealanders (57%), British participants (56%), and Germans (51%) accessed cybersecurity training at work. A third of Americans (33%) and Germans (33%) reported accessing training at home, while French participants (23%) were more likely to access training in a public location
- **Mandatory Training**: Completing mandatory cybersecurity training at work or a place of education was highest among British participants (88%) and lowest among French participants, with almost a quarter (24%) reporting cybersecurity training as a non-mandatory exercise
- **Training Engagement and Preferences**: New questions about training engagement and preferences, such as delivery style
- **Usefulness and Engagement**: Most people rated cybersecurity training as useful (84%) and engaging (78%), whether they had done it at home or work
- **Behavior Change**: Seventy-nine percent of participants reported having put the cybersecurity advice into action. Training influenced behaviors such as better recognition and reporting of phishing messages (50%), using strong and unique passwords (37%), and beginning to use MFA (34%)