

zivver

Security fatigue and how to overcome it

Investigating the causes
of and solutions to
security fatigue



Introduction

Due to the steep increase in focus on compliance in recent years (GDPR, NIS2, DSA), most organizations are expanding their security and compliance programs, increasing the number of security policies and risk awareness activities.

As a result, employees can experience security fatigue; a sense of being overwhelmed by security policies and an inability or occasional unwillingness to comply with these policies, which can lead to lower levels of security and higher risks for the organizations.

To overcome the risk of security fatigue, organizations should make sure their security policies are proportional, simple and explainable. When possible, awareness of the policies should be ‘offered’ just-in-time.



Context

The global attention for information security is growing. On a daily basis there are headlines about data breaches, ransomware attacks, scams and phishing attacks.

Cyber criminals are effective and innovative, continuously improving their tactics to steal data, money or take over information systems. They exploit newly discovered vulnerabilities and use sophisticated social engineering techniques to take advantage of well-meaning, busy employees. These cybercriminals are also ruthless, targeting critical infrastructure and public sector organizations. Truly, no organization is safe from malicious attackers.

As a consequence, the need for protective measures is growing. Although many organizations have information security on the agenda, government agencies are aware that not enough is being done to protect personal information, critical processes and financial systems. More action is needed to protect citizens, businesses and public sector organizations alike.

To turn the tide, the EU is releasing regulations to force the hand of organizations in upping their game around data protection by implementing more protective measures. Examples of this include the NIS2 and DORA.

Either due to fear of being the next cyber victim or by the necessity to comply with new regulations, more and more organizations are expanding their information security program. Indeed, we see more organizations than ever implementing an increasing number of technical and organizational measures to mitigate cyber risks.

Although many measures can (and should) be technically enforced (such as transport layer encryption or email security protocols) plenty of measures depend on the 'users' – mostly employees. However, security is not an employee's core role. These busy individuals are focussed on providing healthcare to the elderly, for example, or teaching children, or providing municipality services – not 'doing security'.

To make sure these employees know what is expected of them, they are asked to attend awareness sessions and sign off on security policies; and therein the problem lies.

What is security fatigue?

As information security threats are multiplying, security measures are multiplying too. Employees are informed of more threats to watch out for and more security policies to follow, creating additional workflows and distractions for their already busy days.

This is more than likely to have an impact on their job; a simple task like reading a new email can take twice as long as they double check if the attachment is safe before opening it.

As a consequence people start to feel overwhelmed by security.

There are too many risks to consider and/or too many policies to remember. People are left feeling beaten by security, as though they cannot get it right and therefore it does not matter if they try. They are also likely to feel that too many security measures are hindering them in performing their jobs.

The result is “a weariness or reluctance to deal with computer security”¹ and security policies are not (always) followed. It triggers feelings of frustration, tiredness and even hopelessness².

A common example of security fatigue is using easy to remember passwords and/or reusing passwords to avoid being locked out of a business system when a strong password is forgotten.

A study from Harvard Business Review in 2022 found that this behavior is quite common.

“We found that across our sample, adherence to security conventions was intermittent. During the 10 workdays we studied, 67% of the participants reported failing to fully adhere to cybersecurity policies at least once, with an average failure-to-comply rate of once out of every 20 job tasks.”³

So, in short, security fatigue is not about ill intent. People know about security rules and they generally agree that security is important but they fail to comply with said rules in a consistent manner.

1. <https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly>
2. Cram W, Proudfoot J, D'Arcy J, (2020) 'When enough is enough: Investigating the antecedents and consequences of information security Fatigue' Link
3. Harvard Business Review <https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies>

Why is it happening?

There are several reasons why people do not adhere to security policies.

Of course, it can be intentional. An employee may not agree with a policy or is convinced the policy is unnecessary and therefore ignores it deliberately.

However, it can also be unintentional. For example, if an employee is not aware of the policy and thus fails to adhere to it. This could also be a consequence of there being too many policies to keep track of.


But research shows that, most of the time, the real reason is somewhere in between.

People are aware of policies and of the threats they are intended to prevent, but their attempts to adhere to them are inconsistent.

While security is top of mind for security professionals, for the majority of employees, they are first and foremost focussed on productivity and getting their job done. If the security measure is making it harder to complete a task, the professional will view the measure negatively, and in an attempt to strike a balance between security and productivity, the 'wrong decision' is made.

The employee may simply mis-assess the risk. They may think that what they are doing is simply not interesting for cyber criminals and assume they or their organization will not be targeted. They may wrongfully conclude that the information that they are handling is not valuable or sensitive.





On the other hand, there are factors that put a lot of pressure on employees to be productive and efficient, resulting in stress overload. Deadlines, increased workflows, or even external factors outside of work may also result in employees feeling as though they have no alternative but to navigate around security measures to get things done quickly.

The desire to help a co-worker, patient or client can also result in violating a security policy. The above mentioned study from Harvard Business Review also found that

“Around 18% of policy violations were motivated by a desire to help a co-worker.”

Of course, employees may also get frustrated. Security measures are often perceived as annoying and sometimes extremely hindering people's work. Some may feel out of proportion or even unnecessary.

Research comparing security fatigue with decision fatigue shows that the quality of decision making and the level of self-control decreases when more decisions need to be made in a row⁴. If users are 'asked' to make many security decisions during their workday they are more likely to make a poor decision.

4. Cram W, Proudfoot J, D'Arcy J, (2020) 'When enough is enough: Investigating the antecedents and consequences of information security Fatigue' [Link](#)

Impact

Security fatigue has a direct impact on the organization. It negatively affects not only security but also, in some cases productivity.

Lower security

Usually the impact of security fatigue is the reduced effectiveness of the security measure in place. As a consequence, the risk mitigation is less effective and the organization might be more vulnerable to data breaches or compromise. In general security fatigue can result in employees ignoring security policies and employees implementing workarounds.

In some unfortunate cases, this may result in:

- The installation of malware because a warning was dismissed
- Credentials are stolen because phishing training was skipped
- Data is shared with unauthorized individuals because a colleague asked for them
- Weak credentials are breached via a brute force attack because a short password was chosen

Lower productivity

But security fatigue can also have a different impact.

The risk of doing something wrong and breaching policy or causing a security incident may also have a paralyzing effect on employees.

In these cases, employees may postpone tasks they perceive as 'risky' or avoid them all together. They may, for example, ignore an email because it might be phishing, or delay sending an important file to a colleague because they are unsure of the relevant security protocols around their communications platforms.

Solutions

Security professionals do not want to cause security fatigue but they also cannot prioritize security policies. After all, security policies are not put in place because it is fun but because it is necessary either to secure the organization and/or to be compliant with security standards and legislations.

Still, there are few things that can be done to lower the risk of security fatigue.

Proportional (right size) security

When implementing a new policy it is key to balance the security gain versus the productivity loss.

It is important to find the right balance and avoid excessive risk avoidance in which the organization is unwilling to accept any residual risk.

For most organizations this will have a crippling effect on their productivity and eventually on the results the organization can achieve.

Make sure security policies are based on a risk assessment; understand which risks are acceptable to your organization and which are not.

Keep security simple

When it has been decided a security policy is needed, ensure it is easy to follow for your employees. This means no difficult decision trees or processes to follow. It should be crystal clear what is expected of employees.

It can also help to integrate security policies within existing workflows so it is impossible to 'forget the security step'.

In addition, the communication around policies should be 'easy' to receive, meaning no lengthy documents full of jargon.

Limit and help with security decisions

Limit the number of 'security decisions' employees need to make. For most employees it is perceived as stressful if they have to make a security assessment to decide if they can or cannot do something; for example, opening a risky looking email. In addition, research into decision fatigue has found that the more decisions that need to be made, the lower the quality of these decisions.⁵

When assessments have to be done by an employee (if, for example, the decision depends on the context), offer support in making these decisions – for example, technology that indicates if and why an email has clear indicators of phishing or malicious payloads.

5. Cram W, Proudfoot J, D'Arcy J, (2020) 'When enough is enough: Investigating the antecedents and consequences of information security Fatigue' Link

Explain the why

Although not all employees will be interested in the reasoning behind security policies, it generally helps to explain why a policy is being introduced or adjusted. Security policies should have a clear purpose for their adoption; explaining the risk that is mitigated and the possible impact on the organization or individual if the risk were to materialize paints a picture for employees, including their role in the organization's security.

Just in time

Many security teams are sharing information around policies via annual awareness sessions, digital training programs and documentation. They may also ask the employees to sign off on policies to ensure compliance and accountability. The problem with this is that people tend to forget a big portion of what has been communicated. It is therefore wise to repeat the message frequently.

It is even more effective if the policy or guideline is also shared just in time, meaning in the moment the employees need to be aware of it.

For example, a pop-up that warns employees they may be visiting a malicious website or is about to download a movie or video game, or a warning that sensitive information was found in an email attachment.

When employees are alerted to a risk or an organizational policy in the right moment, they are more likely to comply and/or do the right thing. The right moment is the moment at which they can immediately use that knowledge to make the right decision. This also lowers the burden of having to remember multiple different rules and regulations, consequentially making the security and compliance program more effective.

The most efficient way to provide timely awareness is by using smart software. A security team may not be able to warn all employees of every danger while they are executing their jobs, but software can.



Zivver vs. security fatigue

Zivver is a tangible example of how a tech solution can counter security fatigue while maintaining the right level of security.

Zivver Secure Email platform protects outbound emails by enhancing email clients with advanced security measures including advanced encryption and multi-factor authentication.

Zivver protects information at a level that aligns with its sensitivity. This means that rather than enforcing encryption and extra authentication requirements to every email sent, the security measures are only enabled when the information in the email (including attachments) is indeed sensitive. This is keeping 'security' proportional to the risk.

To simplify processes for users, Zivver integrates with existing email clients meaning employees do not need to use separate portals or applications to send a secure message. This means they don't have to change their ways of working to add an extra layer of security when needed.

Zivver scans messages to detect sensitive information; if sensitive data is detected, the user is informed instantly, enabling them to take appropriate action before pressing 'send'. For example, Zivver recognises and notifies users to the presence of healthcare information or financial data. As a result, the user understands why an email should be encrypted and can do so with one click. This in-the-moment notification also allows an employee to remove sensitive information from the message if they did not intend for said data to be sent. After all, failure to redact sensitive data remains one of the leading causes of data loss, according to the ICO.

Most importantly, to avoid security fatigue, Zivver alerts users just in time. When an email is written, the employee is made aware of the policy and the risks associated with that specific email, and provides clear direction for the appropriate actions to be taken.

Conclusion

Increasing security policies sees the phenomenon of security fatigue growing. As a consequence, well-intentioned employees are unable to keep pace with their organization's security requirements, undermining their effectiveness and productivity.

To avoid security fatigue, teams must ensure their policies are proportional and simple. They must avoid overwhelming employees with security decisions by explaining the why beyond security policies and, where possible, by providing important policy information just in time. To support their organization in keeping pace with today's growing security threat landscape, it's time to leverage innovative software to support people in making the right security decisions.





London

5 New Street Square
EC4A 3TW London
United Kingdom

+44 (0) 203 285 6300

Amsterdam

Spaklerweg 52
1114AE Amsterdam
The Netherlands

+31 (0) 85 01 60 555