DAYBLINK

Technical Controls as a Driver of Cyber Culture

By Christa Zubic, Nick Suarez, and Steven Schmitz

December 2021

Introduction: What are Forced Technical Controls?

Most sophisticated cybersecurity organizations have embraced technical controls as a management mechanism. Some organizations have even begun mandating their adoption. Forced technical controls, if integrated appropriately into the culture, can dramatically increase cyber defense capabilities as well as combat employees' inherent resistance to change. While proactively initiating change may seem counterintuitive to creating a strong culture, when implemented correctly such a policy underpins and enables the desired behaviors. Required change is efficient and direct, providing employees with less ambiguity and faster results. Forced technical controls, such as Multi-Factor Authentication or Password Managers, paired with an optimized use of employee cyber awareness training can reduce organizational security risk exposure.

The easiest way to conceptualize forced technical controls is to break it down into two parts: 'forced' and 'technical controls.' Let's start with 'forced.' At face value, the word implies employees may be coerced to act or work in a manner with which they may disagree. However, the concept is actually quite common in organizations. Simply put, 'forced' requirements refer to any controls put in place by the organization that employees must fulfill in order to maintain employment status. During employee onboarding, employees are asked to install cybersecurity software and use approved email addresses. Other examples include submitting timesheets, signing Non-Disclosure Agreements (NDA). In short, every organization has policies and procedures that employees are expected to comply with as a requirement of employment.

'Technical Controls' are most often hardware or software that is used to safeguard against bad actors or outcomes. These too, are commonplace across organizations, but they might not be as prevalent in the day-to-day lives of each and every employee. An example of a technical control most organizations have is a firewall, which monitors and filters incoming and outgoing network traffic.

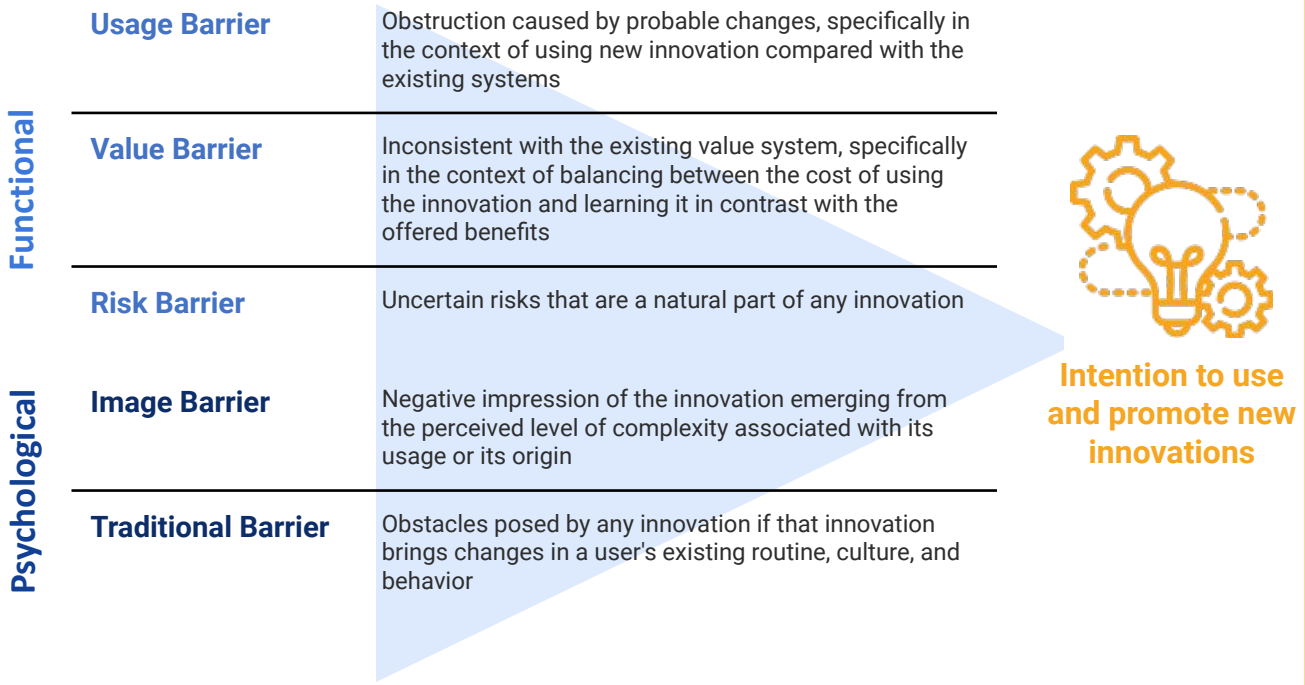
Joining the terms together we have *Forced Technical Controls*' or requirements of employment to safeguard against bad actors or outcomes. When applying a cybersecurity lens to this definition, forced technical controls can include any cyber security best practice that the organization chooses to implement as a formal policy or procedure. Effectively, they are controls put in place to protect both employees and organizations from the errors that most commonly result in data breaches. In addition, they are controls that affect employees mid-stream rather than at the onboarding phase. Organizations can leverage such controls to strengthen their cybersecurity posture, alter employee behavior, and reduce the risk of human error.

Forced Technical Controls Combat Change Resistance with Minimal Time and Costs

Cybersecurity organizations have a responsibility in protecting the information and assets across each function of the business. Despite that responsibility, the budget for security functions sits at about 10% of the IT budget for most organizations.[3] While 10% of the budget may seem reasonable, it is becoming more challenging for several reasons. First being, the cost of developing up-to-date and effective security education materials has reached an all-time record for large enterprises — $290,033 per year, which accounts for time and effort employees put into the preparation and delivery of security training.[4]

[3] "Cybersecurity Budgets Explained" https://triadanet.com/cyber-security-budget-calculator/. Accessed 28 November, 2021.
[4] "Cost of User Security Training Tops $290K Per Year" https://www.infosecurity-magazine.com/news/cost-of-user-security-training/ Accessed 28 November, 2021.
[5] "Puneet Kaur, Amandeep Dhir, Naveen Singh, Ganesh Sahu, An innovation resistance theory perspective on mobile payment solutions, Journal of Retailing and Consumer Services, Volume 55,2020,102059, ISSN 0969-6989, https://doi.org/10.1016/j.jretconser.2020.102059.

Figure 1: The five innovation resistance barriers each have a level of impact on the overall acceptance of new innovations



Source: https://www.sciencedirect.com/science/article/pii/S0969698919307465

Not only does this preparation of this material take significant time and effort, it also takes time away from revenue-generating work as all employees sit through training, which is not accounted for in the value above. However, with limited costs also come challenges with employee sentiment.

When implementing forced technical controls, it is important to understand and anticipate employee sentiment to the pending organizational change. Researchers have named this resistance phenomenon: change resistance theory. In short, innovation resistance among employees is defined as behavior resulting from rational thinking and decision-making regarding innovation because of potential changes that may affect the existing status quo or beliefs [5]

Introducing Forced Technical Controls is a great first step to strengthening cybersecurity culture in an effective, cost- and time-efficient manner. Furthermore, NIST suggests that the first round of technical controls chosen for implementation should be simple, with little disruption to day-to-day work activities, to allow employees to acclimate to the changes. Through the gradual introduction of technical controls, organizations launch an effective cybersecurity posture. In addition, this opens opportunities for expanding the program in the future, depending on KPIs that gauge both employee satisfaction with the cybersecurity program and overall cybersecurity knowledge.

[6] "How Yahoo Built a Culture of Cybersecurity" https://hbr.org/2021/09/how-yahoo-built-a-culture-of-cybersecurity?ab=hero-main-text Accessed 15 July 2021
[7] "Creating a Culture of Security" https://www.nist.gov/blogs/manufacturing-innovation-blog/creating-culture-security Accessed 28 November, 2021.

Forced Technical Controls Remove Organizational Weak Links

Over the past year, the rapid increase in hybrid work environments, resulting from the COVID-19 pandemic, has been cause for great concern among many cybersecurity departments. The quick transition resulted in little-to-no time to pressure test new policies and procedures, and required organizations to be reactive rather than proactive. Coupled with reduced oversight into employee security behaviors and fewer opportunities for real-time feedback or training, organizations are seeing more and more predictable human errors. While strong password hygiene may seem obvious to cybersecurity professionals, research suggests that, despite greatly increased cybersecurity support and investment, there is a lot of room for improvement. A study conducted by the

Figure 2: Employee Routine Cyber Risk

Commuter Risks

26,000 devices accidentally left on the London Tube annually[1]

Coffee Shop Risks

69% of man in the middle cyber attacks occur at public WiFi Hotspots[2]

Written Risks

About 38% of people continue to write down passwords in notebooks or post-its[3]

Sources: https://www.helpnetsecurity.com/2018/07/17/london-transport-lost-devices/; https://www.comunicaffe.com/study-finds-unsecured-coffee-shop-wi-fi-is-particularly-high-risk; :https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security

Figure 2: Shows the three risks to company security that employees face in their typical everyday routine.

A Harris Poll found that 24% of password users still leverage basic passwords such as qwerty, 123456, or password123.[9] In another study conducted by Logmein, it was found that employees reuse their passwords an average of 13 times.[10] The actions in both examples are avoidable and could be made obsolete through forced technical controls that are readily available. To address this concern, organizations should consider introducing Password Managers as one of the forced technical controls. Password managers are an effective and simple technical control that have proved effective at organizations. They allow employees the ability to create more complex passwords that don't need to be remembered; the passwords will be stored within the password manager software. What this means for users is that each and every one of their passwords can be different and complex, without the burden of remembering dozens of unique passwords. With less than half of the companies in the world instituting password managers, there is opportunity to introduce Password Management as a solution to human error and predictability in password choice [11].

[8] "Human Behavior is 93% Predictable, Research Shows" https://cos.northeastern.edu/news/human-behavior-is-93-predictable-research-shows/ Accessed 15 November 2021

[9] "The United States of P@ssw0rd$" https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf Accessed 28 November 2021.

[10] "Impressive Password Statistics to Know in 2021" https://hostingtribunal.com/blog/password-stats/#gref Accessed 15 November 2021

Another forced technical control organizations should include is Multi-Factor Authentication (MFA). MFA requires users to have multiple types of authentication such as a password (something you know) and secondary approval from a different device or account (something you have), to gain access. A LastPass study found that only 57% of companies use MFA when it comes to securing businesses [12]. MFA is a great first-step to implement during a cultural change to a secure organization because it is a control available in products most organizations are already using, G-suite and Microsoft Office and is promoted to protect against 99.9% of automated attacks [13]. These MFA technologies are included in the package companies purchase for these systems, meaning there is no additional cost associated.

As organizations look to enhance their cybersecurity practices, it is important to remember that employees may be their weakest links but they are also their most valuable asset. Maintaining employee buy-in and support, especially when it comes to security training, is difficult. To combat resistance, organizations should focus on the low effort, higher reward mentality that Password Managers and MFA provide - the upfront effort for employees is of great value to the organization as a whole and does not place a heavy burden on the employees [14]. In many instances, Forced Technical Controls are viewed by employees as less burdensome than lengthy security training and are often easier to visualize the downstream organizational impacts. Not only will this quell any frustrations employees may have from security training, but it will also provide some comfort to security teams knowing that technology can be used as an aid to secure the daily routines of employees.

Implementing Forced Technical Controls

Cultural Change is difficult both for organizations and employees. Employees often have a steep learning curve, and organizational leadership has to be willing to work with them through that time of change. For organizations, there needs to be a defined strategy for how the implementation will take effect. For a successful transformational change, there need to be desired outcomes, an integration plan, and continued feedback from those affected by the change. For employees, they need to be aware of the changes through effective communication, they need time to adjust, and need to feel heard. Forced technical controls are an effective way organizations can increase their culture of security. It is, however, a transformation that will require work. Organizations need to be prepared for initial pushback from their employees. Despite that pushback, benefits greatly outweigh drawbacks. When implemented correctly, forced technical controls provide a more secure cyber foundation for the organization, reduce time and energy spent on security training, and can even improve employee perspectives on the importance of cybersecurity awareness. Through thoughtful implementation, organizations will take their cybersecurity cultures to the next level with forced technical controls.

[11] "The 2020 State of Password and Authentication Security Behaviors Report" https://mms.businesswire.com/media/20200219005336/en/773763/5/191522-Ponemon-Infographic-2020-final-1.jpg?download=1 Accessed 2 November 2021

[12] "Global Password Security Report" https://www.lastpass.com/state-of-the-password/global-password-security-report-2019 Accessed 28 November 2021.

[13] "Two-factor authentication statistics: A good password is not enough" https://dataprot.net/statistics/two-factor-authentication-statistics/ Accessed 5 November 2021

[14] "Why Your Employee Training Is A Waste Of Time And Money -- And What To Do About It" https://www.forbes.com/sites/groupthink/2015/08/30/why-your-employee-training-is-a-waste-of-time-and-money-and-what-to-do-about-it/?sh=47a0e25128cf Accessed 5 November 2021

Figure 3: Implementing Forced Technical Controls

PASSWORD MANAGER SOFTWARE

Computer program that allows users to store, generate, and manage their passwords for local applications and online services; only requires the memorization on a single complex password for access to all passwords saved within the manager

Associated Risks

- Weaker passwords may still be used by owners, just saved within the password manager
- A single complex password to access all passwords runs the risk of forgetting the single master password

Mitigation Strategies

- Provide the staff with Password Management training materials, and complex password creation
- Provide training on strategies for memorizing the master complex password used for access

MULTI-FACTOR AUTHENTICATION (MFA)

Technology that requires the users to provide a minimum of two verification factors from a separate device or account to gain access to a resource such as an application, online account, or a VPN; these can be in the form of different applications, codes, etc.

Associated Risks

- Increase in employee resistance due to a more intensive log-in process and multiple device management
- Additional equipment used, some of which may be personal, that may not be as secure as company issued

Mitigation Strategies

- Establish a cultural norm within the company through events such as Cyber Fairs and awareness programs
- Identify champions outside of the Cyber department that will encourage the use of MFA

STRONG PASSWORD MANDATES

Policy or mandates that require a certain character count, numbers, symbols, etc. for password guarding company-sensitive information. These should be standardized across the entire organization to ensure there are as few vulnerabilities as possible.

Associated Risks

- Without well thought out mandates, the enforcement of password complexities could reduce effectiveness
- Mandates could leave employees feeling a lack of trust from leadership on their security practices

Mitigation Strategies

- Updated password requirements within the user setup experience, to prompt adoption of complex password
- Communicate password statistics, specifically common passwords / patterns users should avoid using

Figure 3: Shows the risks and associated mitigation strategies to implementing three technical controls: strong passwords, MFA, and Password Managers

ABOUT THE CONTRIBUTORS

Christa Zubic is a Consultant within DayBlink's Organization & People Center of Excellence and is based in the Vienna, VA office.

Nick Suarez is a Consultant within DayBlink's Cybersecurity Center of Excellence and is based in the Vienna, VA office.

Steven Schmitz is a Consultant within DayBlink's Cybersecurity Center of Excellence and is based in the Vienna, VA office.

For more information on DayBlink's Organization and People services, please reach out to our practice lead, **Rory Teeling (Rory.Teeling@DayBlink.com).**

For more information on DayBlink's Cybersecurity services, please reach out to our practice lead, **Michael Morgenstern (Michael.Morgenstern@DayBlink.com).**

ABOUT DAYBLINK

Today's rapidly changing business environment imposes significant needs for novel solutions and transformation across every sector. Organizations need to adapt for the future of work. We create value for clients by aligning human capital and business value chains through more effective and technologically empowered people, processes and data.

DayBlink is more than a consulting firm. We believe in a better version – of work, of life, and of the future. We combine consulting, entrepreneurship, and philanthropy to make a greater impact on clients' businesses, employees' development, and society. Connect with us to learn more.

Copyright © 2021 DayBlink Consulting, LLC. All rights reserved.