Highlights

Preventing Data Loss in Multinational Companies: Two Case Studies on Phishing Simulation Techniques and Drive Encryption

Martina Bonora, Andrea Ceccon, Leonardo Maccari

- A large-scale phishing simulation campaign carried out in a multinational firm (62.000 sent emails) reports that 6% of the links were clicked by the receivers and 11% of the attachment were opened
- Business and Human Resource topics are the ones that receive more clicks
- A large-scale deployment of disk encryption using Microsoft BitLocker was carried out in a year span, together with other security upgrades.
- At the end, 83% of the computers were successfully configured with BitLocker, only about 59% were also configured with SecureBoot using the trusted platform module hardware.
- Proper scheduling, communication and data dashboards are key to the success of implementing security measures in large-scale companies with thousands of employees.

Preventing Data Loss in Multinational Companies: Two Case Studies on Phishing Simulation Techniques and Drive Encryption

Martina Bonora[a], Andrea Ceccon[b], Leonardo Maccari[a]

[a] *Ca'Foscari University of Venice, Italy*
[b] *University of Innsbruck, Austria*

Abstract

This paper presents two case studies from multinational firms with thousands of employees, each implementing distinct but complementary security measures to prevent data loss. The first case study examines a phishing simulation program that involved sending tens of thousands of simulated phishing emails over the course of a year. The second case study explores the deployment of Microsoft BitLocker disk encryption across thousands of PCs, offering a detailed analysis of the rollout phases and associated challenges.

Both case studies yield valuable scientific insights. The phishing simulation revealed that over 6% of phishing links were clicked, and an alarming 11% of malicious attachments were opened by users. Meanwhile, the BitLocker deployment highlighted that approximately 10% of PCs in a large firm could not be upgraded due to hardware obsolescence.

In addition to sharing new data, this paper details the experiences, obstacles, and strategies encountered during both initiatives. Despite the different contexts, the common lessons learned and shared strategies offer practical guidance and best practices for multinational firms undertaking similar transformations in their security processes.

1. Introduction

Cybersecurity has been a prominent focus of computer science research for the past two decades. However, the scientific literature lacks studies detailing practical experiences in applying security measures within real-world work environments. Bridging this gap is a critical challenge because, out of the many technical solutions proposed to enhance IT security, only a few prove to be viable in practice. Understanding how established firms implement security measures in real-world settings is an essential starting point for designing effective and secure technologies. In particular, data loss is a prominent threat to business continuity, and it can take place due to many technical reasons.

This paper presents the experiences of two

large multinational firms, referred to as Alpha and Beta, in the attempt to minimize data loss across two distinct cybersecurity domains. In both cases, one of the authors was embedded in the firm, monitoring the processes, collecting data, and contributing to the research.

The first case study focuses on Alpha's efforts to combat email phishing, a well-known and persistent security threat [1]. Despite existing countermeasures, industry reports continue to highlight phishing as a major source of data breaches[1]. While phishing simulation campaigns and training are common countermeasures, there is limited data on their effectiveness in real-world organizational contexts. This study documents a 13-month phishing simulation campaign that involved sending nearly 62,000 emails to employees. The findings include insights into the campaign's effectiveness, the topics most likely to trigger risky user behavior, lessons learned, and the actions taken by Alpha. These results are valuable for researchers exploring the effectiveness of phishing simulations and for practitioners seeking benchmark data to evaluate their campaigns.

The second case study examines the technical and organizational processes involved in Beta's rollout of the Microsoft BitLocker disk encryption feature across its PC fleet. BitLocker, a Microsoft Windows feature that encrypts a PC's filesystem [3], safeguards data against loss and theft. However, deploying BitLocker at scale requires meeting specific hardware and software requirements, making the process challenging. Beta's experience, involving approximately 3,000 PCs, is analyzed to identify difficulties encountered, lessons learned, and strategies implemented. These insights are particularly valuable for large-scale organizations planning similar projects and offer a benchmark for assessing the readiness of their infrastructure for secure hardware and operating systems.

The two case studies are complementary, as large-scale firms must implement both types of measures to secure their IT infrastructure comprehensively. Moreover, despite the risks related to data loss, security policies are often perceived as an obstacle to productivity, and it is hard to convince the management and the employees to adopt them. Therefore, despite the technical differences between the two case studies, the paper addresses them jointly because we found strategies that were effective in both scenarios, which are discussed as best practices.

The contribution of this paper is then twofold:

- We provide new data on the effectiveness of phishing simulation campaigns and the technical readiness to implement disk-level encryption.
- We outline best practices that proved successful in both scenarios and can be reused when redesigning security policies in large-scale organizations.

The remainder of this paper is organized as

[1] See the Anti-Phishing Working Group's reports, an industry consortium dedicated to combating phishing activity [2].

follows: Section 2 reviews the state of the art, highlighting the lack of practical use cases in both areas. Section 3 introduces the two case studies at a high level. Sections 4 and 5 present the findings from Alpha and Beta respectively, detailing the results and the technical details of the processes. Sections 6 and 7 report on the lessons learned in the two firms, and Section 8 synthesizes the best practices we can extract from both experiences. Finally, Section 9 concludes the paper.

2. State of the Art

Compared to the technical research papers in the cybersecurity field, published case studies are a very small minority. Here we review some of the works that are available to highlight the differences with our paper. We start with papers describing the enforcement of security processes in firms, then we focus on the ones dealing with phishing and the (very few ones) dealing with data encryption.

2.1. Enforcing Security Policies

Several works focus on the adoption and testing of specific company high-level policies and report the results of surveys with employees of companies in a certain sector. It is the case of Faizan et al. that explored a framework to enhance information security policy compliance among oil and gas company employees, and verified it through surveys [4] or, in a more hands-on approach of Shukla et al. that present a quantitative framework for evaluating and selecting cloud services, focusing on security assurance [5]. Their goal is to help organizations assess and choose cloud providers based on defined security metrics. Also Ahmad et al. focus on internal company policies for incident response, based on surveys to the members of the security operations center of a company [6]. Similarly Bartenes et al. [7] try to better understand the challenges faced when performing IT security preparedness exercises, which are key to improve the response process during a real incident. They designed a multiple case study with six teams in three organizations and collected results with semi-structured interviews. Weishäupl et al. provide empirical contributions to study how firms' investments in information security are decided, showing that there is a lack of consistency across firms and that the security process is perceived to impact the business process in a disturbing way [8]. Dhillon et al. analyse the way the "security culture" is preserved during a merger of two companies. Merges can disrupt the prevalent security culture, thus making the new organization highly vulnerable [9]. These works describe the process of designing security policies in various situations among firms and show that there is a need for empirical evidence to support the management and to motivate the efforts required to enforce those policies. Our paper provides a detailed report on the experiences, the impact, and the results of the adoption of security policies in large multinational firms, and it is beneficial for both researchers and decision makers.

2.2. Phishing

The problem of phishing is well known and it has been explored and analysed in all its

aspects [10], not only the technical ones, as it is known that the human factor is recognized to be a point of failure [11]. Thus, countering phishing with specific training is a research trend that has received considerable interest in recent times and is part of a more general *cybersecurity hygiene* approach [12]. Very recent works like Frati et al. [13] propose methodologies based on surveys and interactions with security experts of healthcare, the methodology is tested through interviews. Similarly, Oruc et al. [14] develop a training framework that is specific for the employees in the maritime industry, with training modules and expert supervision. Also Angafor et al. report on a proof of concept experiment with 50 remote workers that were interviewed and trained with regards to several aspects of security [15]. Brunken et al. [16] report on the hidden costs of phishing simulation campaigns in a firm but do not report on the simulation data. In general, these works approach the phishing problem from a different perspective, which is not data-based like our own approach.

A recent survey collected the papers that we consider more similar to ours, as they are based on phishing campaigns [17]. Among them we mention four works that we consider more related, as their scale is comparable to our experiments, involving a number of emails in the order of tens of thousands. The first one is by Lain et al. [18], which was the first large-scale analysis of phishing simulation campaigns in a real firm. The second and third ones are by Sutter et al. [19] and by Yeoh et al. [20], which collected data on a large user base, but in a completely different setting (university students and employees). Finally, Hillman et al. [21] evaluate phishing simulation in a company together with training. Our paper confirms some of the findings in these works and extends the literature with an in-depth analysis of the phishing topics that collected the largest number of dangerous actions.

2.3. Data Encryption

Data encryption is, of course, a massively studied subject; however, practical experiences on applying available technologies to existing firms have been rarely documented in the literature. We mention Kim et al, [22] that report on a database encryption technology used for compliance with Korean laws, while You and Xiao estimate the cost of encryption with a simulation approach [23]. More attention has been dedicated to experience in using encryption with e-mail communications [24, 25] and in general, there are many works that focus on the usability of encryption techniques [26], but not on the process of introducing disk encryption in a large firm. Breivik et al. report on a security migration plan of a Windows-based company, however, the plan does not include the adoption of BitLocker, being a cloud-based migration [27]. Other studies like Hasan et al. [28] focus on the dependency and the design of a repeatable methodology for enforcing post-quantum cryptography, but do not report the detailed experience with it in a real use case.

Our work extends and complements the existing ones as it provides insights on some under-explored factors, it reports details of

the process adopted by the companies, it provides findings on a scale that is two orders of magnitude larger than typical small scale surveys, it provides suggestions and best practices for both researcher that want to develop new security frameworks, and practitioners that are about to start the same process in their company.

3. Introduction to the Case Studies

Alpha and Beta are multinational companies spread around the world, with thousands of employees. Alpha is in the beverages sector, and Beta is in the fashion sector, so neither of them has a specific focus on IT, but, of course, IT permeates their business processes. Alpha and Beta markets are divided into main geographical areas: Europe, Middle East, Africa, Americas, and Asia-Pacific. Alpha is present in 27 countries, Beta in 30. The headquarters of both firms are in Italy.

There are several reasons why the two companies decided to engage in the described security activities, the first one being a general increased awareness about the cybersecurity risks that grew among the company management. Another important factor was compliance with the international privacy regulation. Specifically, in the Beta company, a security audit revealed that to be compliant with several international laws, it was necessary to harden the security features of the computers that process the personal information of customers and employees. Among these laws, we mention:

- The *General Data Protection Regulation (GDPR)* in Europe, which has set a high standard for data protection
- The Brazilian *General Data Protection Act*, known as the *Lei Geral de Proteção de Dados*, is a data protection law that came into effect in 2020, modeled closely after the European Union's GDPR.
- The Japanese *Act on the Protection of Personal Information (APPI)*, is designed to safeguard the personal information of individuals, created to regulate the handling of personal data by businesses and government agencies.
- The South Korean *Personal Information Protection Act (PIPA)* governs the processing of personal information in South Korea and includes provisions related to consent, data subject rights, data security, and cross-border data transfers.
- Singapore's *Personal Data Protection Act (PDPA)* requires stringent measures to ensure the security of personal data.

If a multinational company decides to enforce only one technical configuration for all its chapters, it must respect the most stringent law requirements among the possible ones.

Another factor that influenced the management was the implications of insurance. The management reported that insurance providers increasingly require proof of robust data protection measures as a prerequisite for coverage. By implementing upgrades and security measures, a company demonstrates its

commitment to prevent data breaches, which can lead to more favorable insurance terms and lower premiums, as described in previous works [29].

3.1. Specific Motivations for Alpha

Alpha used a platform specialized in cybersecurity awareness training, distributed as eLearnings. In most of the cases, eLearnings courses do not last longer than 15-20 minutes and present many animations, quizzes, and interactive activities to engage the user. The eLearning videos used by Alpha were already available on the platform and not created ad hoc for the firm. They provided an overview of some common cybersecurity topics, including phishing, malware, the use of personal devices, and data leaks. The training was mandatory for new employees but it had to be followed only once in their career in Alpha.

Training sessions are time-consuming and are perceived as an additional cost by the management and an added burden by the employees. In order to practically test their efficacy and justify their need and their further planning, phishing simulation campaigns were introduced on a monthly basis. The results were used as a basis to plan the new training activities. We report on the effectiveness of the campaign and the lessons learned by the management.

3.2. Specific Motivations for Beta

To align with GDPR and other regulatory requirements and enhance overall data security, the company planned a comprehensive compliance project. The cornerstone of the project was to implement BitLocker in order to provide full disk encryption to safeguard sensitive information across all company devices globally, even if the hardware is compromised.

However, a number of other security functions were also included, as a requirement for BitLocker or as added features. All of these became part of the company's upgrade strategy and introduced some specific challenges. We report on the success rate, the time-evolution of the upgrade, and document the obstacles encountered during the project, which can be common to other firms. As an example, some of the roadblocks were artificially introduced by the licensing scheme of Microsoft products, which forced the firm to implement a one-size-fits-all scheme. Documenting this experience provides prior knowledge to those who need to design an IT infrastructure and need to compare the Microsoft ecosystem with other systems, such as open-source alternatives.

4. Case Study 1: Alpha Vs Phishing

Phishing simulation involves sending simulated phishing emails to employees (including executives) to see how they behave. These emails typically mimic legitimate messages but contain links or attachments designed to trick recipients into disclosing sensitive information or performing actions that compromise corporate security. Phishing simulations help organizations identify vulnerabilities in their employees' knowledge and behavior related to cybersecurity and provide input for improving the effectiveness of the training.

4.1. Simulations in Alpha

Every month, Alpha's employees received a randomly chosen simulated phishing email from a subset of more than 300 templates on 4 difficulty levels. The templates were mostly generic ones, but they also included references to the firm itself (i.e. they directly included the firm name). The difficulty expresses the level of concealment of the phishing email, from 1 (the email is poorly crafted and easy to classify as phishing) to 4 (the email is carefully crafted and requires a high effort to be classified as phishing), the higher the difficulty, the higher the similarity to the service they impersonate. The various templates, together with the difficulty levels, were included in the software used for the campaign. Emails were dealing with different trending topics, such as banking and finance, Human Resources (HR), Business, and many others. Emails were in English and were not tailored for the specific country where the employees were residing, so that employees were subject to the same content. Emails coming from outside the organization were tagged as such by the email servers, but the spam filters were disabled for the study.

Employees were able to report a suspicious email using the specific Microsoft Outlook button "Report as Phishing". Once reported, the email was then examined and a feedback, whether negative or positive, was sent to the employee. There were three types of "*hooks*" in the emails: links to be clicked, attachments to be opened, or QR codes that the user could scan with their mobile phone. Whenever a user interacted with the hook (e.g. by opening an attachment, clicking, or scanning the QR code), the action was detected by the platform, and the user was added to an additional bi-weekly campaign. In the bi-weekly campaign two more simulated emails were sent to verify if the employee was keen to fail again or not. Alpha tracked progresses and failures monthly, developing internal reports to enhance its strategies. The reports focused on the number of recipients, the number of emails opened, the number of failures, and the number of emails reported as phishing, divided by geographical region. Information related to sex, gender, and age was not taken into account in the reports. Note that not all the data we show refers to the same period of time, as the configuration of the platform used for the phishing simulation campaign was modified during the test period, providing a growing level of detail.

We analyse the period from February 2023 to February 2024, which was used by the management to evaluate the overall training strategy. We outline the results, the difficulties, and future initiatives that were inspired by this activity.

4.2. Results

Table 1 reports the overall total numbers of emails sent, emails opened by the employees, and the number of failures for each month. A failure is any action that can lead to a security breach, like clicking on a link, opening an attachment, or scanning a QR code. QR Code Phishing (or Quishing) is a type of phishing attack that uses QR codes to trick people into visiting a malicious website or downloading a virus-filled document. Fig. 1

graphically reports the percentage of failures per month.

There is a declining trend up to September 2023 and then a steep increase, with another decrease in the last month of analysis. The reason for this behaviour is that in fall 2023, due to a decrease in the phishing-prone percentage, Alpha decided to increase the difficulty of the simulations, using templates extremely similar to legit emails and, therefore, difficult to identify as phishing cases. This required employees to pay attention and examine the email carefully before trusting its content. The main goal of this decision was to prevent employees from getting used to the campaigns and to lower their attention level. Indeed, the data confirm that phishing training campaigns need to be periodically renewed or they become ineffective.

Table 2 reports the overall failure rate and reported emails, split in the three regions

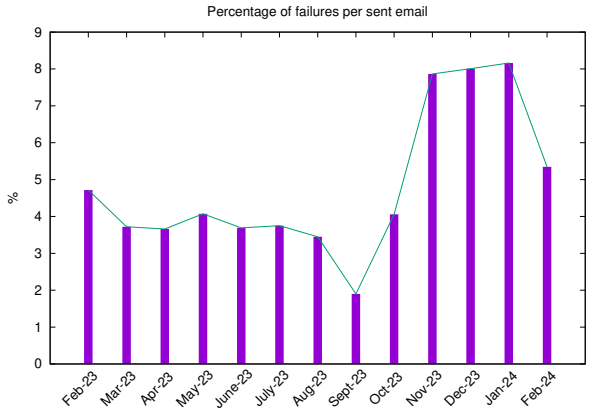

Figure 1: The ratio of failures for each month in the period Feb-2023 - Feb-2024.

Month	Sent Email	Opened	Failures
Feb-23	5047	1694	238
Mar-23	5430	1669	201
Apr-23	5027	1641	183
May-23	5232	1528	212
June-23	5283	1570	194
Jul-23	5386	1615	202
Aug-23	4669	1591	161
Sept-23	4158	1283	79
Oct-23	4288	1515	174
Nov-23	4336	1781	341
Dec-23	4371	1841	350
Jan-24	4374	1798	357
Feb-24	4395	2391	235
Total	61996	21917	2927

Table 1: data collected from February 2023 to February 2024 about the emails sent each month, the total of these emails opened by employees, and the number of failures detected. Note that one email can produce more than one failure (e.g. click on a link and download the attachment) but it is counted only once.

where the firm has employees. We see that there is a small, not significant fluctuation in the overall failure rate by region and a larger difference in the number of reported emails, but not really correlated with the failure rate. The percentage of reported emails is below 30%, which shows that there is not a strong interest in reporting fake emails.

Table 3 reports the actions. The IT team in Alpha was able to track the specific action performed, divided by region. Note that this table reports the absolute numbers because we don't have the information about the total number of sent emails divided by their hook (link, attachment, QR code) for the whole

	EMEA	AMERICAS	APAC
Overall failure rate (%)	6.6	6.4	7.7
Reported emails (%)	29.39	19.30	24.91

Table 2: A breakdown of failure and reported emails per region. Each number reports the percentage on the whole period (Sept. 2023 - Feb. 2024).

period, but only for the two months that we reported later. This is due to the fact that the tool used was modified during the campaign to expose more information to the IT staff of Alpha. Note also that the phishing emails were sent in English language regardless of the region. The large majority of the failures were related to clicking on a fraudulent link. This is an action that is (wrongly) considered at a lower risk, and users tend to do it even if in doubt about the email's legitimacy. Even more worrying is the fact that a very large number of employees, even after having received a training, opened an email attachment. In the considered period, a total of 357 attachments were opened, a number that represents an important threat for the firm. Scanned QR codes represent a small minority of the actions.

Table 4 reports the relative failure rate split by kind of action. In this case, the number is normalized over the overall emails sent with each specific content, so the percentage represents the number of e.g. clicked links, over the total email containing a link to be clicked. The percentage can then be considered as a kind of effectiveness of each threat vector. Note that the number of emails sent in this table is higher than what is reported in Table 1 for the corresponding months because a single email can carry more than one malicious content and trigger more than one failure. In that case, it is counted more than once. This dataset is available only for the last two months. Compared to Table 3 we see that the tendency of clicking on a link or scanning a QR code is similar, however the relative data also confirm that email attachments are an alarming threat, as they show the highest effectiveness. The percentage of clicked links is surprisingly very close to the one reported by Lain et al. [18] in a similar setting (5.6%), and [20] in a higher education setting (5.5%) which suggests a generic trend that can be used as a baseline for future experiments and other firms.

The last data we report is the correlation between the topic of the phishing email and the percentage of failure. Table 5 reports the failure rate by topic normalized by the number of sent emails for that topic. The topics and their distribution were automatically decided by the platform. Among the topics that received the highest number of emails the Business and Human Resources categories largely outperform the other topics. The technical topics (IT, Mail Notifications) are also among the topics that people tend to fail more. There are some very specific ones that have high percentages but

Action	EMEA	AMERICAS	APAC
Links clicked	1255	938	325
Attachment opened	171	148	38
QR code scanned	28	25	3

Table 3: A breakdown actions. Each number reports the raw number of actions (Feb. 2023 - Feb. 2024).

Action	Emails with Hook	Failures	(%)
Links clicked	7965	508	6.38
Attachment opened	1252	138	11.02
QR code scanned	204	14	6.68

Table 4: The failure rate for different types of actions (Jan. 2024 - Feb. 2024). The first column describes the action that can lead to a failure, the second the number of emails that contained content that could be the target of the action, third and fourth columns the number and percentage of failures.

an overall smaller number of emails, so they might reflect some topic that, besides being a niche topic, targets people that have a higher risk of being victims of phishing (Retired Events, Real Estate).

5. Case Study 2: Beta Vs BitLocker

Enforcing BitLocker disk encryption has its own requirements, and Beta considered this to be the right occasion to enforce other desirable security features. The first is the transition from legacy BIOS to UEFI, a mandatory element of the compliance strategy. UEFI provides a more secure booting environment and supports modern security features that are not available in legacy BIOS systems. Unlike the legacy BIOS, UEFI supports larger hard drives, faster boot times, and Secure Boot activation. Secure Boot ensures that only trusted software runs during the system startup process, safeguarding the integrity of the boot process. Operating system (OS) updates to (at least) Windows 10 version 1809 were required as this specific version is needed to activate and manage BitLocker through Microsoft Entra ID (formerly Azure Active Directory), ensuring seamless integration with the company's encryption policies.

However, not every computer was ready to be upgraded, due to hardware and software requirements. In particular, Secure Boot needs specific hardware prerequisites to ensure optimal functionality: key parameters include the firmware version of the Trusted Platform Module (TPM), which must be at least 2.0. The disk configuration must use the GUID Partition Table (GPT) instead of the Master Boot Record (MBR) to support UEFI, which requires GPT's support for large disks, numerous partitions, and redundant partition tables, ensuring also the com-

Topic	Emails	Failures	%
Online Services	1865	60	3.22
Business	1708	171	10.01
IT	1605	79	4.92
Human Resources	1502	176	11.72
Holidays	408	13	3.19
Banking	347	4	1.15
Social Networks	296	4	1.35
Mail Notifications	266	15	5.64
Coronavirus	206	10	4.85
Seasonal	159	2	1.26
QR Code	99	4	4.04
Current events	85	3	3.53
Government	58	1	1.72
Healthcare	44	1	2.27
Real Estate	35	3	8.57
Legal	30	0	0.00
Retired events	26	3	11.54
Education	19	1	5.26
Local Language	16	1	6.25
Data Breach	13	0	0.00

Table 5: The percentage of failures divided by topic (Jan-Feb 24).

patibility with BitLocker's encryption protocols, as BitLocker relies on GPT's ability to create necessary system and recovery partitions and integrates with UEFI's Secure Boot feature. Moreover, configuring TPM ownership to the system rather than the user allows the operating system to manage access securely. Ownership to the system means that the operating system, rather than an individual user, holds the authority to control the TPM, ensuring that the TPM's security functions, including key storage and encryption, are governed by the system's security policies and remain unalterable by individual users. In this way, the system can autonomously handle key generation, storage, and recovery, integrating with features like Secure Boot.

5.1. Deployment Process with SCCM

Finally, once the OS was updated, the user account to which the device is registered must have the Microsoft 365 F3 license.

The deployment of BitLocker leverages the System Center Configuration Manager (SCCM), a Microsoft tool for overseeing large groups of computers, to streamline the process. This method ensures that each PC meets the necessary requirements before initiating the process. Once the PCs have been categorized based on the actions that need to be taken, another instrument, Microsoft Intune, will be used to push the necessary upgrades and configurations.

PCs are initially registered on the SCCM console and classified into three specific collections based on the requirements they meet:

- TPM firmware version must be version 2.0 or higher

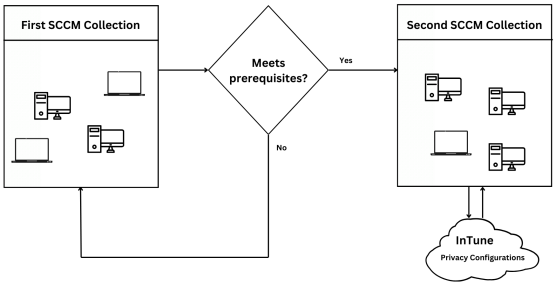

Figure 2: Steps and Procedures for the deployment

- TPM ownership must be assigned to the system
- The disk must be configured using the GPT partition scheme

The time it takes for a PC to move from the initial collection to the second one and start the encryption can vary. Typically, it takes a couple of days for a PC to pass all these checks, provided that the PC remains powered on and in use within the company's network (or with the use of VPN). This time frame allows the system to perform a deep assessment and communicate the results back to the SCCM console. Two days to perform a relatively simple system check may seem a surprisingly long period, but in real conditions, there are several factors that influence the process, such as the constant availability of Internet connection and VPN set-up, and system reboots due to user behavior. This time must be taken into account by the IT team dealing with the process.

If a PC passes these initial checks, it is automatically moved to a second collection within SCCM. This collection is configured

to download commands from SCCM, indicating that the PC has met the prerequisites, and it can download and enforce the security policies from Microsoft Intune. After receiving these commands, the PC enters a waiting state until Intune delivers the configurations. This waiting period can range from one hour to up to seven days, depending on various factors, including network conditions and system workload because, since Intune is a SaaS platform, its responsiveness can be affected by system overload and other external factors, which further emphasizes the need for stable and continuous network connectivity and consistent uptime during the deployment and encryption phase to ensure the completion of the whole process.

5.2. Results

The BitLocker implementation project was divided into distinct phases, starting with the headquarters (HQ) deployment and then extending to the outlets and boutiques. Over seven months, the company aimed to encrypt all its PCs around the world, for a total of 3341 machines. We will see that this was not possible.

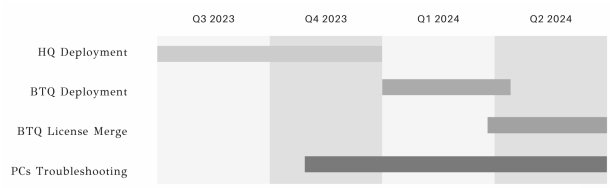

Figure 3: BitLocker deployment timeline for both the Head Quarter (HQ) and Boutiques (BTQ).

The deployment project was centrally coordinated from the central HQs, which were responsible for both the deployment strategy and the ongoing monitoring of the project. This involved overseeing the configuration setup and ensuring that all procedural steps were updated and followed accurately. Weekly documents were sent out to regional IT teams, detailing the current wave of machines scheduled for encryption and providing all the guidelines to fix the machines that could not be automatically encrypted during that wave. These guidelines provided updates and troubleshooting instructions, ensuring that all relevant stakeholders were aware of the upcoming encryption activities and prepared for the associated operational impacts. Moreover, for hardware and BIOS interventions, such as switching from legacy BIOS to UEFI mode or upgrading TPM chips, on-site interventions in the boutiques were delegated to external suppliers, which played a crucial role in handling tasks that required physical presence and specialized technical skills.

5.2.1. Phase 1: Headquarters Deployment

The initial phase focused on deploying BitLocker across almost 2,000 HQ PCs over five months. This phase was multifaceted, involving three parallel efforts: updating operating systems to meet the requirements for Entra ID, deploying BitLocker on machines that already met these prerequisites, and refreshing hardware by replacing PCs that lacked a TPM.

- *BitLocker Deployment*: More than 1000 machines were already compliant with

the requirements and moved to the encryption phase.

- *OS Updates*: BitLocker in *Entra ID* requires at least the Windows 10 1809 version, and at that time, approximately 900 machines had a previous version (1507), necessitating a bulk upgrade.
- *Hardware Refresh*: About 10% of the PCs did not have a compliant TPM chip and were replaced.

By the end of the five-month period, 1,600 machines at the HQ were fully encrypted, with the remaining 400 machines scheduled for follow-up due to various minor issues such as software incompatibilities or user availability. This means that in a relatively controlled environment (compared to the computers in the boutiques), only 50% of the computers were ready to upgrade, 45% needed a software upgrade, and 10% a hardware upgrade (with non-void intersection between the two last groups).

5.2.2. Phase 2: Boutiques Deployment

Following the HQ deployment, the focus shifted to the boutiques, where the deployment was completed within two months, targeting around 1300 machines. This phase was particularly challenging due to the need to update the operating systems, which could have led to conflicts with the boutique's point-of-sale software, however, it benefited from the experience gained in the HQ. To mitigate potential disruptions, the updates were executed in small, weekly waves of 100 to 150 machines, distributed evenly across all regions. This method ensured that, after updating, the machines in a waiting state could begin downloading configurations from Microsoft Intune and start the encryption process. This gradual approach was crucial to parallelize the efforts and avoid disruptions to the boutiques' daily operations, thereby ensuring business continuity. Table 6 reports the time progression of the number of encrypted PCs by month, both in the HQ and the boutiques.

Date	**HQ**	**Boutiques**
August 2023	250	0
September 2023	350	0
October 2023	400	0
November 2023	375	0
December 2023	225	0
January 2024	25	450
February 2024	40	560
March 2024	10	20
April 2024	5	10
May 2024	25	20
June 2024	5	10
Total	1710	1070

Table 6: Number of Encrypted PCs by month.

Table 7 reports the progress state up to when the process was monitored (Jun 2024) with a breakdown of the actions successfully completed. We see that the OS upgrade was

successful in 94.8% of the cases, as this is the action that has the lowest set of requirements. UEFI upgrade was also possible on more than 90% of the PC as most of the modern hardware platforms allow it. BitLocker was successfully configured, and the disk was encrypted on roughly 83% of the PCs, while SecureBoot was the step that had the lowest success rate, as it was possible in slightly less than 60% of the PCs.

Overall, enforcing BitLocker is easier than SecureBoot, which proved to be more challenging due to the higher requirements (hardware and software) that it needs.

6. Lessons Learned at Alpha

This section reports the main lessons learned during the processes and the actions that the firm's management decided to take to support its success.

6.1. Improving Security Perception at Alpha

The strategy adopted by Alpha until February 2024 allowed the company to build the foundations of cybersecurity culture and awareness over the years, but it presented some weaknesses as well. The main one can be linked to the frequency aspect: the eLearning was considered mandatory only for new joiners, meaning that the employees had to complete it compulsorily, but only once and during their first days within the company. This entailed people not only to consider the topic not important enough, but also to forget about it during the years. The second one is related to the strategy obsolescence, as people got used to the phishing hooks but failed to recognize them when the difficulty increased.

Three actions were taken to improve the situation: new and improved eLearning courses tailored for the company profile, a cybersecurity booth at the company's annual conference, and a bot that enables continuous interactions with the employees.

6.2. New eLearning Platforms

A new eLearning platform was created from scratch following the company's graphical guidelines. The training covers most of the themes present in the previous version, but also new ones such as Artificial Intelligence (AI), deepfakes, and social media. The training script is aligned with the needs of Alpha, including ad hoc instructions such as how to properly report a phishing email or which social media employees are allowed to use. Corporate-approved platforms have security mechanisms that analyze and filter messages, sending an alert if some come from a suspicious and potentially dangerous source (e.g. Microsoft Teams shows an alert message when a person outside the organization is trying to send a message. In this way, employees are warned to pay attention when opening a chat with an external person, as it might be a phishing attempt).

The eLearning includes some use-cases set in the company environment so that employees can identify themselves in the scene. It is translated in different languages, increasing the compatibility with all employees around the world that might not be familiar and comfortable with English. The training becomes mandatory for all employees and not only the

Upgrade	Number of PCs	(%)
Operating System Upgrade	3168	94.8
UEFI Upgrade	3015	90.2
BitLocker Deployment	2780	83.2
SecureBoot Activation	1969	58.9

Table 7: Project Advancement at Q2 2024

new joiners and is recommended to be attended more than once during the career path of each employee. The creation process is still ongoing and the final version is expected to be working by the end of 2024, and evaluated in 2025.

6.3. Cyber Security booth

Every year Alpha hosts a global convention, which is attended by its general managers, directors, and C-levels from all over the world. In 2024, the cybersecurity team had the opportunity to set up a desk at the entrance of the convention room. In order to engage employees to come at the desk, some activities were developed. Two monitors were installed, one looping cybersecurity awareness videos about phishing, remote working, and other themes, and the other one showing real-time attacks that were mitigated by Alpha's security systems.

In addition, people had the possibility to check on the HaveIbeenpwned[2] website whether their email address had been subject to data breaches or not. The website collects publicly available databases of breached emails, and if a match was found, the platforms, the year of the attack, and the type of information stolen (e.g. email, password, birth date) were shown. While checking the corporate email and the private one, if desired, the security team was available to discuss the results and answer any kind of doubt. Once checked, people were asked to fill out a brief survey about cybersecurity awareness and best practices. At the end of the convention 142 responses were collected.

Among the questions asked, we report the answers to the question "*How much prepared do you consider yourself when talking about cyber security best practices?*". Among the interviews, 17% responded "very prepared", 65% reported themselves "somewhat prepared", 9% chose "neither prepared nor unprepared", 8% "somewhat prepared", and 1% selected "very unprepared". As the survey was filled out after checking the email breach, many people reassessed their self-evaluation, often lowering the score. In addition, employees with a compromised email asked for suggestions and next steps to protect themselves and also their families from these data breaches.

6.4. Cybersecurity Bot

To reduce the effectiveness of phishing attacks, the idea of a cybersecurity bot was introduced. The bot would serve as a digital

[2]See `https://haveibeenpwned.com/`.

assistant to share cybersecurity best practices with employees who have risky digital behavior, i.e. any kind of email-related action that was detected and could expose the individual or the organization to some security threats. This concept was defined in the security policies adopted by the company. The bot was developed by an external provider. Its functioning is simple: once connected with the security systems adopted by Alpha (primarily intrusion detection systems), it sends a notification either via email or via Microsoft Teams as soon as a risky or suspicious activity is detected. Messages can be managed and personalized in the provider's platform, and they contain a text and an infographic with best practices related to the action that was detected. Text and image are constraints imposed by the tool provider. If one of them is missing, the configuration cannot be completed successfully.

The first step taken by the team to start the project was to identify the main scenarios and the associated detection rules for which notifications had to be sent. Detection specifies types of activities, anomalies, or patterns within a dataset or network traffic that require attention. The cybersecurity team chose phishing, malware, risky login, and data breach as main scenarios to be covered. For instance, if a rule detected a click on a potential phishing email, it would then send to the employee via the bot the best practices associated with phishing.

7. Lesson learned at Beta

Several roadblocks or generic difficulties were encountered in the implementation of BitLocker at Beta, which we report and document in this section.

7.1. Handling Legacy Systems

The deployment of BitLocker involved significant manual interventions, particularly for older machines that were not automatically compatible with the BitLocker prerequisites. Besides hardware requirements, a critical issue was the need to switch the BIOS from legacy mode to UEFI mode, which was delegated to external suppliers who visited the boutiques to perform the necessary changes. First the BIOS settings were accessed, and the boot mode was changed from legacy to UEFI. After switching to UEFI mode, the system's disk partition style had to be converted from MBR to GPT. Once the BIOS and partition changes were completed, the operating system was reconfigured to boot in UEFI mode. In the boutiques, due to the critical nature of the point-of-sale software, there was apprehension about updating Windows 10, as any disruption could severely impact sales operations. Consequently, the updates were rolled out in small, incremental waves, coordinating every week with the team in charge of the point-of-sale software.

7.2. Problems with Microsoft licenses

A critical challenge in deploying BitLocker within the boutiques was related to licensing issues. For BitLocker to function correctly, PC users needed to be integrated with

Intune, which required a Microsoft 365 F3 license. Initially, the boutique systems relied on multiple shared accounts for different activities (e.g., sales, email, stock management), all of which were used by the same group of employees. However, none of these accounts held the appropriate license for device enrollment, and purchasing a Microsoft 365 F3 license for each of these accounts for every boutique would have been prohibitively expensive. To resolve this, the fragmented shared accounts were merged into a single shared account per boutique with the necessary F3 license, allowing the devices to be enrolled in Intune and receive the required security configurations. This restructuring enabled the PCs to receive the required security configurations from Intune, allowing the encryption process to proceed.

Due to the complexity and scale of this operation, the process lasted about two months, extending beyond the initial BitLocker deployment timeline. The consolidation of licenses not only resolved immediate encryption issues but also facilitated future projects, such as the rollout of mobile devices in boutiques. In fact, with properly licensed accounts, boutiques could now register devices like iPads or shared iPhones in Intune.

However, the new configuration has a less fine-grained user privileges segmentation, and this specific roadblock highlights how vendor lock-in can introduce significant delays due to licensing issues.

7.3. Failed Encryption

About 100 computers had a recurring problem caused by attempts to encrypt the disk that were interrupted or failed, leaving the disk in an inconsistent state. This was due to reboots triggered by the users or some other software failure. To address this problem, an operator had to connect to the PC remotely using a remote access software, then decrypt the disk, restart the PC, ensure the TPM configuration was correct, and restart the encryption.

8. Learning from the Case Studies: Best Practices to Enforce Security Policies

We report here a few of the best practices matured during both projects. Even if they are general, we consider them insightful to guide other practitioners in avoiding the same problems and streamlining the process of enforcing policies against data loss.

- **Improve the Overall Security Perception:** Changing a process is perceived as a cost by the employees, so it is fundamental to motivate them and incentive their participation. The survey and the booth used in Alpha were key to justify the added workload due to eLearning activities.

- **Clear and Simple Troubleshooting Guidelines:** Develop comprehensive, yet simple troubleshooting guidelines that can be easily accessed and understood by multi-cultural local IT teams around the world, ensuring that common issues can be resolved quickly and efficiently. Employees should not

feel that they don't know what to do when they receive a phishing email or when their terminal does not behave as usual due to an ongoing security upgrade.

- **Engage Different Stakeholders and Create War Rooms:** Engage all relevant stakeholders and offices, including IT teams, external consultants, and business unit leaders, from the beginning. Moreover, establishing war rooms, dedicated spaces for addressing critical issues, can facilitate rapid problem-solving and minimize the impact on daily operations. It also helps to design the depth of some actions that can be perceived differently by the IT team and by other teams. We mention, for instance, the level of personal information collected during phishing campaigns in Alpha, or the re-organization of accounts in Beta.

- **Adopt a scalable phased approach:** Implement the project in phases, starting with a pilot phase to refine processes and identify potential issues, allowing for the creation of the project's guidelines and adjustments before scaling up. This step-by-step approach improved the training/testing process in Alpha and allowed a smooth upgrade in Beta.

- **Regular and Effective Communication:** Maintain regular communication between the central coordination team and regional IT teams with periodic updates. These reports help ensuring everyone is on the same page and prepared for upcoming tasks. Moreover, they motivate the management to push security policies, countering the perception of them being an unnecessary cost.

- **Clear visual dashboards:** Integrating data into graphical dashboards can provide clear insights and facilitate effective tracking of the process. This was key in Alpha to visualize the effectiveness of the phishing campaign and to provide feedback to users, and in Beta to follow the progress of the migration. In both cases, the presence of an easy-to-use monitoring graphical tool was essential. Graphical analysis is particularly important in the communication with the upper-level managers, that require only key information to back the security processes from within the management.

- **Detailed Planning and Resource Allocation:** Ensure detailed planning and resource allocation, particularly for activities that involve significant involvement of people (new phishing campaigns in Alpha, or manual interventions/hardware upgrades in Beta).

9. Conclusions

Security measures in large firms are constantly updated and re-evaluated, as their effectiveness changes with time. It is of paramount importance for researchers who design those measures and practitioners that apply them to have access to previous experiences, and to update their course of action

based on them. This paper contributes to the description of two case studies in which key data was collected about two security measures adopted to mitigate data loss: phishing simulation and encryption of entire drives on PCs using the Microsoft Windows operating system. On the one hand, we provide a valuable scientific contribution, confirming some of the results obtained by previous studies and extending the insights with new evidence. On the other hand, we describe all the required steps, the process that the companies adopted, the time it took, and the difficulties encountered. Based on the described experience, we also discuss the common best practices that helped the success of both the processes, and are of paramount importance for any firm that is about to start a similar effort in enforcing a new security policy.

References

[1] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, J. Porras, Mitigation strategies against the phishing attacks: A systematic literature review, Computers & Security 132 (2023).

[2] Anti Phishing Working Group, Activity january-march 2024 (2024).
URL `https://apwg.org/trendsreports/`

[3] C. Tan, L. Zhang, L. Bao, A Deep Exploration of BitLocker Encryption and Security Analysis, in: IEEE International Conference on Communication Technology (ICCT), 2020.

[4] R. Faizan Ali, P. Dominic, S. Hina, S. Naseer, Fostering information security policies compliance with ISA-95-based framework: an empirical study of oil and gas employees, International Journal of Information Security 23 (2) (2024).

[5] A. Shukla, B. Katt, M. M. Yamin, A quantitative framework for security assurance evaluation and selection of cloud services: a case study, International Journal of Information Security 22 (6) (2023).

[6] A. Ahmad, S. B. Maynard, K. C. Desouza, J. Kotsias, M. T. Whitty, R. L. Baskerville, How can organizations develop situation awareness for incident response: A case study of management practice, Computers & Security 101 (2021).

[7] M. Bartnes, N. B. Moe, Challenges in IT security preparedness exercises: A case study, Computers & Security 67 (2017).

[8] E. Weishäupl, E. Yasasin, G. Schryen, Information security investments: An exploratory multiple case study on decision-making, evaluation and learning, Computers & Security 77 (2018).

[9] G. Dhillon, R. Syed, C. Pedron, Interpreting information security culture: An organizational transformation case study, Computers & Security 56 (2016) 63–69.

[10] R. Goenka, M. Chawla, N. Tiwari, A comprehensive survey of phishing:

Mediums, intended targets, attack and defence techniques and a novel taxonomy, International Journal of Information Security 23 (2) (2024).

[11] Hamidreza Shahbaznezhad, Farzan Kolini and Mona Rashidirad, Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter?, Journal of Computer Information Systems 61 (6) (2021).

[12] A. A. Cain, M. E. Edwards, J. D. Still, An exploratory study of cyber hygiene behaviors and knowledge, Journal of Information Security and Applications 42 (2018).

[13] F. Frati, G. Darau, N. Salamanos, P. Leonidou, C. Iordanou, D. Plachouris, E. Syrmas, E. Floros, G. Nikitakis, G. Spanoudakis, K. Kalais, S. Tsichlaki, E. Damiani, G. C. Kagadis, J. Najar, M. Sirivianos, Cybersecurity training and healthcare: the AERAS approach, International Journal of Information Security (2024).

[14] A. Oruc, N. Chowdhury, V. Gkioulos, A modular cyber security training programme for the maritime domain, International Journal of Information Security (2024).

[15] G. N. Angafor, I. Yevseyeva, L. Maglaras, Securing the remote office: reducing cyber risks to remote working through regular security awareness education campaigns, International Journal of Information Security (2024).

[16] L. Brunken, A. Buckmann, J. Hielscher, M. A. Sasse, "To do this properly, you need more Resources": The hidden costs of introducing simulated phishing campaigns, in: USENIX Security Symposium, 2023.

[17] N. Marshall, D. Sturman, J. C. Auton, Exploring the evidence for email phishing training: A scoping review, Computers & Security 139 (2024).

[18] D. Lain, K. Kostiainen, S. Čapkun, Phishing in organizations: Findings from a large-scale and long-term study, in: Symposium on Security and Privacy (SP), 2022.

[19] T. Sutter, A. S. Bozkir, B. Gehring, P. Berlich, Avoiding the hook: Influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception, IEEE Access 10 (2022).

[20] W. Yeoh, H. Huang, W.-S. Lee, F. Al Jafari, R. Mansson, Simulated phishing attack and embedded training campaign, Journal of Computer Information Systems 62 (4) (2022).

[21] D. Hillman, Y. Harel, E. Toch, Evaluating organizational phishing awareness training on an enterprise scale, Computers & Security 132 (2023).

[22] Y. S. Kim, E. K. Hong, A Study of UniSQL Encryption System : Case Study of Developing SAMS, in: International Conference on Advanced Communication Technology, 2007.

[23] B. You, X. Xiao, Data encryption technology application in enterprise cost operation management based on cloud computing, Soft Computing (2023).

[24] C. Stransky, O. Wiese, V. Roth, Y. Acar, S. Fahl, 27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University, in: Symposium on Security and Privacy (SP), 2022.

[25] A. Lerner, E. Zeng, F. Roesner, Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists, in: European Symposium on Security and Privacy (EuroS&P), 2017.

[26] S. Ruoti, K. Seamons, Johnny's Journey Toward Usable Secure Email, IEEE Security & Privacy 17 (6) (2019).

[27] S. Breivik, G. K. Dvergsdal, E. Ø. Sørli, Centralizing security and operations of windows clients in an emergency care it infrastructure, B.S. thesis, NTNU (2021).

[28] K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, M. McKague, A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies, IEEE Access (2024).

[29] S. A. Talesh, Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses, Law & Social Inquiry 43 (2) (2018).