

Nalah Kirkendall

Global Business

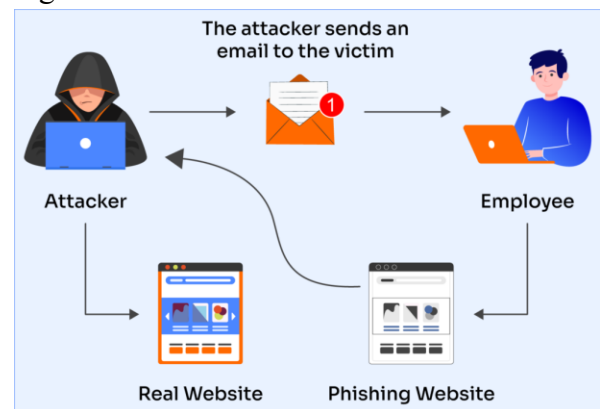
17/10/2025

Integrating Cybersecurity into Corporate Strategy: Challenges and Imperatives

Technology advances every day, as a result the threat of viruses, hackers, and other threats to businesses increases too. That's why cybersecurity should be a priority for any kind of business. Especially when it comes to protecting the customers, employees, and companies' privacy. This discussion focuses on the role of cybersecurity programs in preventing information, data, and financial losses for businesses. Furthermore, we talk about the challenges that come along with finding the right cybersecurity program that fits the needs, wants, finances, and size of the company. To ensure this, a business should effectively integrate cybersecurity while conducting research to avoid repeating common mistakes. This underscores the importance of embedding cybersecurity across all aspects of a business to safeguard against potential threats.

Cyber security has increased in the past decade with businesses working remotely, as well as the increasing amount of businesses marketing on social media. First, we start with the work from home where we started to see the increase of attacks on firms where “1 in 10 firms fell victim to cyber-attacks in 2021,” meaning hundreds if not thousands of businesses all around the UK alone have reported attacks on their business (Fenner-Jamieson, 2022) These stats are just based off of those

companies that had to implement the work from home schedule into their business. Now we have real world incidents that show how damaging these attacks can be for businesses of all sizes. One example of this is the Garmin ransomware attack that had many of Garmin's “online services... interrupted including website functions, customer support, customer-facing applications, and company communications” causing a major shut down for the entire company (Tidy 2020). Not only can an attack like this cost thousands of dollars' worth in sales but millions in recovery fees. Cases like this can disrupt operations, drain resources, and compromise customer trust, putting a strain on business stability. These cases show how damaging cyberattacks can be for businesses operating in a traditional digital environment.



(Phishing Prevention Best Practices: How to Detect & Avoid - Valimail, 2022)

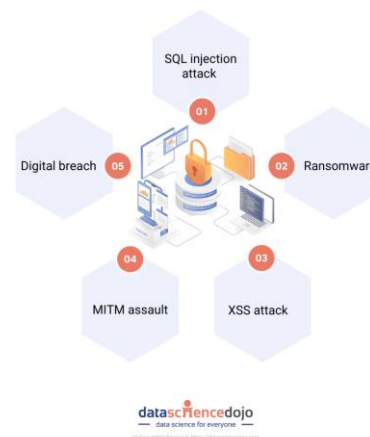
However, as companies increase their use of social media, the risks continue to grow; therefore, implementation of social media in businesses has raised the risk of attacks even higher. There are multiple different ways for a business to get attacked on social media from “phishing attempts, targeting individuals with more detail and higher

accuracy,” which can involve new and financial records that can be used to attack a business (Chin, 2023). So, it became increasingly easier for a cyber-attack to happen on a small business with multiple social media accounts, and the “average cost per attack from loss of money or data [is] \$4,200 for all business reporting an attack” which can really break a small business that is just starting out (Protecting Your Smaller Business from Cyber Attacks | British Business Bank, n.d.). This is just a factor of what some businesses have lost due to cyber-attacks. From cyber-attacks to breaches, these can cause businesses to shut down for weeks at a time. In response, with the growing spread of information about business through social media, comes the growth of cyber security.

Although cyberattacks may not affect every business, this reality does not diminish the need for all organizations to implement robust protective measures. Business can start with an audit, of their business in order to see firsthand what the biggest threat to their company is, “where weaknesses are identified, internal audit can play a vital role in recommending improvement to protect businesses from these fast-evolving threats” that are hard to predict with the naked eye (Insights, 2025). Since cyber security goes on to more than just a defensive program for business software and websites, it's important to incorporate cyber security in all aspects and departments within the business. Thus, businesses need to “take personal responsibility to provide regular training for their staff” so they have the training they

need when growing a business on social media (Insights, 2025). Records such as employees' finances, and personal data are digital assets that can be breached. This sensitive material can be used against the employee or company about sometimes “breaches can go undetected for months; an industry study from IBM found that it takes an average of 258 days to identify and contain a breach” and by then time, money, and data has already been lost (Narang, 2025).

Most common types of data breaches in 21st century



(Data Breaches You Must Prepare for before 2023 | Data Science Dojo, 2025)

This finding highlights that cyberattacks are often not immediately obvious, allowing hackers access for an extended period of time to confidential material on a business before the actual business can act. Therefore, one way for businesses to start incorporating cyber security measures is starting with employees, because when it comes to marketing a business on social media, employees are at the front lines of what is being shared with the audience. This is why it's important for employees to have proper social media and security training

when starting in the business. Employees and businesses should be able to identify sensitive information that should be kept in the walls of their businesses and analyze what the biggest threat is when marketing and working online for a business. This training starts at boardroom level with the “innovative strategies and campaigns, ongoing training, and drills to ensure cybersecurity awareness messages trickle down to the entire workplace” allowing for security to start with the employees first (Chin, 2023). These messages include updates on the evolution of cyber threats and what employees should look out for. Preparing for attacks is only the first step; successfully embedding cybersecurity into corporate strategy requires careful planning and ongoing effort.

The challenge that comes along with integrating cybersecurity into corporate strategy is the training that comes with it. Employees would have to go through training, so they know what to look for when it comes to security risks. Since security threats can be as simple as a “fake email asking users to visit a phony website that steals the data entered,” or malware that “enable(s) hackers to bypass security networks and steal data” it's important for employees to stay cautious on a daily basis when it comes to spreading information (Protecting Your Smaller Business from Cyber Attacks | British Business Bank, n.d.). The challenge that come with training employees is the fact that there is constant advancement of cyber-attacks, making it hard to differentiate a cyber-attack to a normal business email or ad. Consequently,

businesses will need to make sure that employees are able to continue their day to day job while also making sure that they are able to “contain attackers to prevent damage, and to respond and recover when an attack has got through your defenses” because it not only preventing attacks, but recovering from them as well (Ellison & Whitehouse, 2025).



On of UK's top Cyber Security programs (Cyber Essentials Solutions, 2023)

Therefore, it's up to the business to decide where to focus their time and money when it comes to their cyber security. Some businesses may have more weak points than others, so it ultimately comes down to what works for who. Since, business vary in what they sell, how they promote their business, and how much information they are willing to put out into the world about their business; it can be hard to determine what kind of measures businesses needed to incorporate in their business. This is where businesses fail in cyber security because they sometimes “neglect these measures, making it easier for hackers to exploit vulnerabilities” meaning it's easier to take the time and spend the money to protect your business, because in the long run it can be worth it (F24, 2023).



(Employee Training Can Strengthen Your Defense against Digital Threats, 2024)

Ultimately, it's up to the manager and HR to determine what the highest risk is to their company. Now we go onto what businesses should be prepared for after an attack with is incident response which is being able to work through and recover from breaches that may happen within a business, because “even the best defenses can be penetrated” thus plan should be planned for if it does happen in their business (Narang, 2025). Having a clear incident response plan ensures that businesses can respond effectively to breaches, minimizing damage, and maintaining operation stability. Considering the growing cyber risks and challenges business faces, effective cybersecurity measures are no longer optional but essential for protecting both data and operations.

As technology evolves so does businesses, and unfortunately that means the cyber threats that come with it. From hacking, phishing, and data breaches, businesses should make it essential to create a cyber security plan for their business. With the growth in work from home employees, and use of social media in business; the vulnerabilities, and exposure of businesses

become more of a target to attacks. With employees being at the front lines, they play an essential role in preventing and pointing out possible cyber security threats within the business, making the proper training for employees critical for the privacy of the business. However, the integration of cyber security into corporate strategy presents challenges of the evolving cyber-attacks, training requirements of employees who have to take time away from their actual jobs. Then, there is the difference of businesses, making it hard to choose what security system will work for them, where many companies fail to determine where to focus their security investments. To start the business, the need to make an internal audit is key to pointing out the most vulnerable points of the business and then making a response plan to ensure that if the business is attacked or breached, the business will be ready. Without these protections, even a single breach can result in serious loss of finances, information, time, and operation of damage to a company. This is why it's important to have effective cyber security with continuous training, investment, and coordinated planning across all departments to safeguard both business and employee records.

References:

Chin, K. (2023, May 8). *The impact of social media on cybersecurity.*

[Www.upguard.com](http://www.upguard.com).

<https://www.upguard.com/blog/the-impact-of-social-media-on-cybersecurity>

Cyber Essentials Solutions. (2023).

[Itgovernance.co.uk](http://itgovernance.co.uk).

https://www.itgovernance.co.uk/solutions-for-cs-certification?utm_source=bing&utm_medium=cpc&utm_campaign=688890667&utm_content=1283131468304565&utm_term=cyber%20security%20qualifications%20uk&msclkid=6bc3c6d7295a1544cf97aff340a9f52c&utm_source=bing&utm_medium=cpc&utm_campaign=

Data breaches you must prepare for before

2023 | Data Science Dojo. (2025, October 11). Data Science Dojo.

<https://datasciencedojo.com/blog/types-of-data-breaches-2023/>

Ellison, J., & Whitehouse, O. (2025).

Incidents impacting retailers – recommendations from the NCSC.

Ncsc.gov.uk.

<https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers>

Employee training can strengthen your defense against digital threats.

(2024, November 25). BLR.

<https://blr.com/resources/cybersecurity-facts-and-why-training-is-important/>

Fenner-Jamieson, M. (2022, July 21). *How*

Working From Home Has Increased Cyber Threats - Intaso. Intaso.

<https://intaso.co/news/how-working-from-home-has-created-more-cyber-threats/>

F24, T. B. |. (2023, May 15). *Why do*

businesses and organizations fail to prevent cyber attacks?

Www.thebci.org.

<https://www.thebci.org/news/bcaw->

[2023-why-do-businesses-and-organizations-fail-to-prevent-cyber-attacks.html](#)

Narang, J. (2025, March 11). *Why*

Employees Are The First Line Of Defense Against Cyber Threats.

Forbes.

<https://www.forbes.com/councils/forbestechcouncil/2025/03/11/why-employees-are-the-first-line-of-defense-against-cyber-threats/>

Insights, I. (2025). *Cyber security biggest risk as businesses reel from major attacks.* Icaew.com.

<https://www.icaew.com/insights/viewpoints-on-the-news/2025/sep-2025/cyber-security-biggest-risk-as-businesses-reel-from-major-attacks>

Phishing Prevention Best Practices: How to Detect & Avoid - Valimail. (2022, September 28). [Www.valimail.com](http://www.valimail.com). <https://www.valimail.com/resources/guides/guide-to-phishing/phishing-prevention-best-practices/>

Protecting your smaller business from cyber attacks | *British Business Bank.*

(n.d.). [Www.british-Business-Bank.co.uk](http://www.british-Business-Bank.co.uk). <https://www.british-business-bank.co.uk/business-guidance/guidance-articles/business-essentials/a-guide-to-protecting-your-smaller-business-from-cyber-attacks>

Tidy, Joe. “Garmin Begins Recovery from Ransomware Attack.” *BBC News*, 27 July 2020, www.bbc.co.uk/news/technology-53553576.