Celayix

Data Security in the Modern Workplace

Table of Contents

Introduction: The Modern Workplace

The modern workplace is a far cry from previous environments. Private office banks gave way to an open concept, with rooms featuring personal desks encircled by pony walls, hot and hotel desks, and collaboration zones. Covid-19 disrupted workplace and space management, but a return-to-work campaign is developing.

No supervisor wants to discourage employee participation and cooperation. Restoring productivity necessitates the exchange of information and ideas. Whether your office is open, traditional, or a hybrid, a robust set of data and personal privacy regulations is required. For today's modern workplace, there are two major policy types to consider:

Data Privacy Policy
Some employees may require access to sensitive corporate information, such as payroll, intellectual property, and product development plans. Companies should establish explicit policies to guarantee sensitive data is not visible to bystanders. Consider the following options:

- Monitoring privacy screens
- Automatic and lockable screen savers
- Checking in and out of sensitive documents
- Mandatory lock screen requirement
- These are just a few examples of data policies that any tech company or data security company would suggest.

Personal Privacy Policy
Employees will require confidentiality to conduct critical conversations and meetings with clients, vendors, investors, and other stakeholders. Everyday communications should also be evaluated, such as chats with colleagues or personal phone calls. Privacy tools may include the following:

- White noise machines or light music to muffle face-to-face conversations or calls
- Partitions on conference tables and between desks
- Designated areas/rooms for private calls and meetings

While our primary focus in this eBook is to tackle the issue of data security, it is not to suggest that data privacy and personal privacy are two separate notions. Our goal in this eBook is to connect these two notions and emphasize the importance of IT security in the modern workplace.

Section I: Cloud Data Security

What is Cloud Data Security?

Cloud data security refers to the technologies, policies, services, and security controls that safeguard any form of data in the cloud from loss, leakage, or misuse caused by breaches, ex-filtration, and unauthorized access. A solid cloud data security strategy should include the following components:

- Providing data security and privacy across networks, as well as within apps, containers, workloads, and other cloud environments
- Data access control for all people, devices, and software
- Providing total access to all network data

The cloud data protection and security policy must also safeguard all forms of data. This includes the following:

- **Data in use:** Securing data being utilized by an application or endpoint via user authentication and access control.
- **Data in motion:** Encryption or other email and message security procedures ensure the safe transfer of sensitive, confidential, or proprietary data while it moves across the network.
- **Data at rest:** Using access limits and user authentication, data saved on any network location, including the cloud, is protected.

What are the leading cloud security risks?

The majority of cloud security vulnerabilities fall into one of the following broad categories:

- Data has been disclosed or leaked.
- Internal data has been accessed by an unauthorized individual from outside the organization.
- An authorized internal user has too much access to internal data.
- A malicious attack, such as a distributed denial of service (DDoS) attack or malware infection, cripples or destroys cloud infrastructure.

A cloud security strategy's purpose is to mitigate the threat posed by these hazards to the greatest extent possible by securing data, managing user authentication and access, and remaining operational in the face of an attack.

Personal data belonging to more than 100 million Android users was exposed in a 2021 data leak due to misconfigured cloud services.

Checkpoint.com

What are some of the critical technologies for cloud security?

A Cloud security strategy should include all of the following technologies:

1) Encryption
Encryption is a method of converting data into a code so that only authorized parties can decipher it. If an attacker breaches a company's cloud and discovers unencrypted data, the data can be used for various harmful purposes, including leakage, sale, and use in additional attacks. If the company's data is encrypted, the attacker will only find scrambled information that cannot be exploited unless the decryption key is discovered (which should be almost impossible). Encryption, in this way, helps to avoid data leaks and exposure even when other security measures fail.

2) Identity and access management (IAM)
Identity and access management (IAM) products track who a user is and what they are allowed to do, and they approve users and deny access to unauthorized users as needed. IAM is critical in cloud computing since users' identity and access credentials, not their device or location, determine whether they may access data.

IAM mitigates the risks of unauthorized users gaining access to internal assets and authorized users exceeding their privileges. The correct IAM solution will mitigate various attacks, including account takeover and insider attacks (when users or employees abuse their access to expose data).

3) Firewall
A cloud firewall adds an extra layer of security around cloud assets by restricting dangerous online traffic. Cloud firewalls, as opposed to traditional firewalls, are hosted in the cloud and provide a virtual security barrier surrounding cloud infrastructure. This category includes the majority of web application firewalls.

DDoS (Distributed denial-of-service) attacks, malicious bot activity, and vulnerability exploits are all prevented by cloud firewalls. This decreases the likelihood of a cyber-assault destroying a company's cloud infrastructure.

All these key technologies show that technological advancement is key to improving cloud security. But things are constantly changing when looking at cloud security — and, by extension, cloud data security — in the workplace.

Why HR Data Management and Security is Safer In the Cloud

Many organizations experience data leaks, but few are willing to admit it, let alone know how to stop it. According to a survey conducted for IBM last year, the average total cost of a data breach is $3.92 million (USD), with the average price for each lost record being $150. According to the research, these costs have been rising year after year.

Cloud-based third-party providers are intended to protect users, improve data security, and meet privacy legislation requirements. While the key is to choose the right technology, an excellent cloud-based software would ensure:

- Multiple layers of security to Protect Users and the Company
- Mitigate Risk and Improve the Employee Experience
- Achieve enhanced Data security

The second last point brings to the idea of cybersecurity attacks such as phishing and data breaches. The next section of the eBook will discuss the increase in cybersecurity attacks and the need for Data Protection Regulations.

Section II: Cybersecurity Crisis and the Importance of Data Protection Regulations

Cybersecurity Crisis: The Rise of Cyber Attacks

Covid-19 has caused a shift in criminal activities. While the pandemic may have lowered the likelihood of physical crime, such as home break-ins and pick-pocketing, targeted cybercrime is rising as thieves capitalize on public fear of Covid-19. Cybercriminals are changing their techniques and are increasingly targeting people in their homes, which are often also their offices. Companies face heightened cyber risk as working from home becomes a gateway to new forms of data theft. Employees can be a weak link in corporate IT security systems and cybercriminals aim to obtain corporate data, consumer information, and intellectual property.

As the economy grows more digital, the growing cyber danger outpaces most organisations' capacity to properly handle it. Employees' personal information, company data, consumer information, intellectual property, and crucial infrastructure are all at danger. It is still impossible to determine the long-term impact of the Covid-19 problem, but it will undoubtedly have accelerated digitalization in the business environment. At the same time, the cyber threat is growing, and the fact that many employees are increasingly working from home introduces additional hazards.

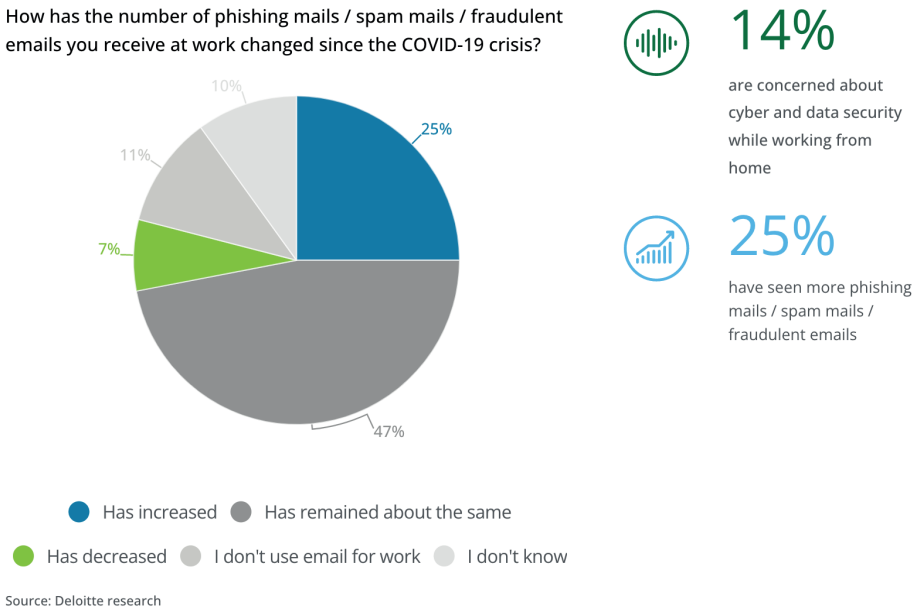
Work from Home

A recent article by Deloitte discusses the risks of working from home due to cyber crimes. It discusses the technological pitfalls of working from home.

Employees that work from the home encounter a variety of hurdles, including missed interactions with co-workers and diversions from partners and family members. They also face issues with technical infrastructure and poor cyber and data protection.

Many governments worldwide instituted lock-downs in March 2020, recommending anybody who could work from home to do so. Many employees first found this appealing because they believed they would be able to manage their time more effectively, have fewer interruptions, work with more focus, and save time by not commuting. However, reality set in quickly as the first few video conferences or attempts to share data with project teams revealed flaws in their IT infrastructure.

Chart 2: Trends in phishing emails and spam since the beginning of the COVID-19 crisis



Source: Deloitte research

It is difficult for non-security experts to estimate their employer's efforts to enhance their IT security. Despite this, 14% of survey respondents are concerned about cyber and data protection when working from home. Furthermore, 25% report increased fraudulent emails, phishing attempts, and spam to their workplace email, with this issue receiving public attention.

The survey findings corroborate anecdotal evidence from businesses that this epidemic has prompted a shift in cybercrime methods as they have followed employees to their new workplaces. Cyber crooks are attempting to exploit flaws in remote IT security measures. Cybercriminals are one of the external risks that security-conscious businesses do not like to face.

Because of the length of the lockdown and its economic consequences, many employees are becoming increasingly concerned about their job security. Many people are motivated to save money if "the worst happens," losing their job, or their company goes bankrupt. So how are employees getting affected by the rise of cyber-attacks?

Cybersecurity Burnout?

According to a new study, nearly one-third of cybersecurity specialists intend to leave the industry when businesses are battling to safeguard their networks against cyberattacks. Why? Burnout.

Burnout may be the most severe cybersecurity issue confronting enterprises in 2022. With the number of data breaches in 2021 exceeding 2020, security teams are under even more pressure to keep firms secure in 2022. However, when strength and resilience are more crucial than ever, burnout, low staff morale, and excessive personnel turnover may put firms at a disadvantage when attempting to manage the growing cybersecurity threat.

Employers are already in difficulty when it comes to cybersecurity in 2022. Not only is the number of attempted cyberattacks increasing globally, but businesses are also under pressure from a tightening labour market and record levels of resignations, all of which are harming the tech industry. Burnout endangers cybersecurity in a variety of ways.

According to 1Password research, the problem of remote working two years into the COVID-19 pandemic leaves employees worn out and less inclined to follow security requirements. The research's key findings were:

- Burnout is a significant issue in the United States and Canada. Research showed that 80 percent of office workers and 84 percent of security specialists are exhausted.

- Burnout is associated with inadequate security practices. 20% of burned-out employees believe their company's security procedures "aren't worth the hassle," compared to 7% of non-burned-out employees.

- People's password choices are influenced by burnout. 12% of burned-out respondents use the same or a few different passwords for everything at work, compared to 7% of workers who are neither emotionally nor physically exhausted.

- Employees that are burned out are more inclined to use IT. Almost half (48%) of burned-out employees reported creating, downloading, or using software at work that their company's IT department had not approved.

- The vast resignation, burnout, and security behaviours are all linked. Employees preparing to resign are more inclined to value convenience over job stability.

- Employees that are ready to resign utilize more shadow IT. 49% of workers wishing to switch jobs use unapproved software, compared to 34% who are satisfied with their current position.

The advent of remote or hybrid working has permanently altered many workplaces, and companies must implement proper cybersecurity strategies to mitigate risk. How do we reduce cybersecurity risk in the modern workplace? Our next section will discuss the importance of data protection regulations and cybersecurity policies!

Data Protection Regulations and Cybersecurity Policy

Many governments consider data privacy a fundamental human right, and data protection laws are in place to defend that right. Individuals must believe that their data will be treated carefully to engage online. Organizations use data protection practices to demonstrate to their clients and users that they can be trusted with their data.

Due to the absence of regulation in data privacy regulations in the United States and Canada, corporations have seized the opportunity to ensure that all parties, whether clients or employees have their data secured. Because there is no federal comprehensive data privacy regulation, most firms use GDPR as a baseline to ensure that their data privacy regulations are compliant and up to date.

GDPR: The EU's Data Protection Regulation, which has gone Viral.

The General Data Protection Regulation (GDPR) is the world's strictest privacy and security law. It imposes requirements on enterprises that target or collect data about EU citizens. On May 25, 2018, the regulation went into effect. The GDPR imposes severe penalties on those who break its privacy and security regulations.

The GDPR signals Europe's hard stance on data privacy and security when more individuals commit their data to cloud services, and breaches are becoming more common. The legislation is big, broad, and vague, making GDPR compliance a frightening proposition, particularly for small and medium-sized businesses (SMEs). So what are the critical regulatory points of the GDPR?

Data Protection Principles
You must meet the seven data protection and accountability principles if you process data:

- ***Transparency, lawfulness, and fairness***: Processing must be legitimate, fair, and transparent to the data subject.
- ***Purpose Limitation***: Purpose limitation entails processing data only for the legitimate purposes specified to the data subject when the data was obtained.
- ***Data minimization***: Data minimization entails collecting and processing only the essential information for the reasons mentioned.
- ***Accuracy***: Personal data must be kept accurate and up to date.
- ***Storage restriction***: You may only keep personally identifying information for as long as required for the indicated purpose.
- ***Integrity and confidentiality***: Processing must be carried out to maintain proper security, integrity, and confidentiality (e.g., encryption).
- ***Accountability***: entails the data controller demonstrating GDPR compliance with these requirements.

Accountability

According to the GDPR, data controllers must demonstrate that they are GDPR compliant. And this isn't something you can do after the fact: if you believe you're GDPR compliant but can't demonstrate it, you're not. You can accomplish this in a variety of ways, including:

- Assign data security duties to your team.
- Maintain complete documentation of the data you acquire, how it is used, where it is stored, who is responsible for it, and so on.
- Train your employees and put in place technical and organizational security measures.
- Have Data Processing Agreement arrangements in place with third-party data processors you hire.
- Appoint a Data Protection Officer (which is not required for all enterprises).

Data Security

You must manage data securely by implementing "appropriate technical and organizational measures." Technical precautions can range from asking your staff to utilize two-factor authentication on personal data accounts to partnering with cloud providers who use end-to-end encryption.

Staff training, including a data privacy policy in your employee handbook, or limiting access to personal data to only those employees in your firm who need it are organizational measures. Moreover, If a data breach occurs, you have 72 hours to notify the data subjects or risk fines.

Data Protection by Design and by Default

Everything you do in your organization must now address data protection "by design and by default." You must consider data protection principles while developing any new product or activity. Article 25 of the GDPR addresses this principle.

Let's say you're launching a new app for your firm. You must evaluate what personal data the app may acquire from users and strategies to reduce the data and safeguard it with cutting-edge technology.

When You’re Allowed to Process Data

Article 6 specifies the circumstances under which it is permitted to process personal data. Don't even think of collecting, storing, or selling someone's data unless you can justify it with one of the following:

- The data subject provided you with specific, unequivocal permission to treat the data. (For example, they have subscribed to your marketing email list.)
- Processing is required to carry out or prepare a contract to which the data subject is a party. (For example, before leasing property to a prospective renter, you must conduct a background check.)
- You must process it to fulfill a legal responsibility. (For example, you may obtain an order from a court in your jurisdiction.)
- You must process the data to save someone's life. (For example, you'll probably recognize this one when it applies.)
- Processing is required to complete work in the public interest or to carry out an official function. (For example, you are a private garbage collection service.)
- You have a genuine reason to process someone's personal information. This is the most adaptable legal foundation, albeit the "basic rights and freedoms of the data subject" always precedes your interests, especially if the data is that of a kid.

Consent

There are new standards in place that define what constitutes consent from a data subject to process their information.

- "Freely provided, precise, informed, and unambiguous consent" is required.
- Consent requests must be "clearly distinguished from other topics" and written in "clear and plain language."
- Data subjects have the right to withdraw consent at any time, and you must respect their decision. You cannot just alter the processing's legal basis to one of the other explanations.
- Children under 13 can only offer consent with their parent's permission.
- You must preserve documentary proof of permission.

People's Privacy Rights

The GDPR acknowledges a slew of new privacy rights for data subjects, intending to give individuals more control over the information they provide to companies. Organizations must grasp these rights to be GDPR compliant.

- The following is a list of data subjects' privacy rights:
- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights to automated decision-making and profiling.

Becoming GDPR compliant is not easy, and it would be easier for companies to create their cybersecurity policy. With remote working becoming more widespread, it might be challenging to think about data security when there is so much more. The GDPR compels businesses to keep personal data safe and secure.

These changing circumstances of working remotely necessitate a different approach to security than when working from centralized offices. Especially when preserving the GDPR-mandated data security, you may help assure GDPR compliance even if your workforce is dispersed by taking a few simple steps. The following and final portion of our booklet will provide complete guidance in developing a cybersecurity policy for your business.

Section III: Creating a Cybersecurity Policy

A cybersecurity policy is the most effective strategy for any firm to safeguard workplace data security. The preceding parts must have established a solid foundation for comprehending the notion of data security and its framework. However, in most industries, the rules and sub-policies may differ. Nonetheless, the following section aims to serve as a model for an organization's IT and HR teams in building their cybersecurity strategy.

Create a Culture of Data Security Awareness

The culture of your firm is crucial to developing an effective cybersecurity posture. Its culture must stress, promote, and drive security-related behaviour. A resilient workforce cannot exist in the absence of a cyber-secure culture.

Mindset
Mindset is an essential aspect of culture. We improve our ability to address cyber hazards by instilling knowledge in the organizational culture. Every organization is vulnerable, whether a small non-profit or a Fortune 100 corporation. Given the ubiquity of cyber threats, we must remain vigilant and prepared. At the individual level, a mindset will promote proper actions, contributing to the resilient workforce that any firm requires.

Leadership
The organization's leaders set the tone. The most significant component in shaping awareness and mindset is leadership. Leaders must adopt cybersecurity education, understanding, and best practices. Leaders must also advocate for security investments and cybersecurity in enterprise risk management. Leaders should not be highly technical but model excellent personal security habits based on established recommendations.

A cyber-secure organization requires leadership participation; your cyber defenders will be able to concentrate on a smaller, more manageable number of problems.

Internal awareness initiatives are another typical technique to develop a cyber-secure culture. Organizations have developed effective ways to generate "buzz" around essential security themes, ranging from posters and newsletters to contests and prize drawings. While these strategies should be used all year, National Cybersecurity Awareness Month in October is an excellent opportunity to stress these themes.

Performance Management
Incentives and disincentives can significantly influence human conduct. Individual performance goals must match organizational goals for cultural change in cybersecurity preparation. Completing needed training, improved reactions to phishing exercises, policy compliance, and avoidance of harmful online activities can all be performance goals for security. Organizations use financial and operational measurements; security metrics should work as well.

Technical and Policy Support
Companies can implement technical controls associated with human behaviour to reinforce cyber-secure culture. Password restrictions, multi-factor authentication, and mobile device management systems can all help to promote a security culture in the same way physical access controls do. An organizational policy can help implement control by explaining the negative consequences of noncompliance.

Leaders can implement these rules in various ways to reflect each firm's distinct culture. They must serve as the foundation for creating a cyber-secure culture by raising awareness and cultivating the proper mindset. With a solid cyber-security culture, each business unit can concentrate on its particular contribution to the organization's protection.

Enforce Email Security

Email security is critical to your company's overall IT security since it is the most prevalent security threat. Phishing emails and fraud are two assaults that require no technical competence, only a grasp of human nature, a flair for deceit, and an email account.
Persuading a person to click on a malicious link is much easier to breach a network than attempting to circumvent its firewall.

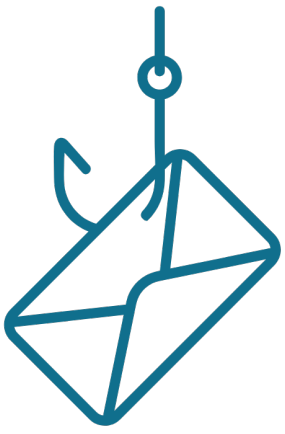
Phishing and fraud are becoming increasingly widespread issues. According to a new threat report by cybersecurity firm Proofpoint, email-based assaults on organizations surged by 476 percent between 2017 and 2018. According to the FBI, these sorts of assaults cost organizations worldwide $12 billion every year.

Email security, like overall IT security, depends on teaching your personnel to apply protection best practices and spot potential phishing efforts. This Enforce email security must be thoroughly engrained in every staff member so that they are vigilant to the danger of hostile behaviour every time they check their emails. In this section, we'll primarily focus on phishing.

Phishing & fraud email assaults costs organizations worldwide $12 billion every year.

Federal Bureau of Investigation

Phishing
By far, the most prevalent sort of IT security attack your company will encounter is phishing. It includes someone impersonating an actual client, institution, or colleague to trick your staff into disclosing critical information, such as corporate financial details and passwords, or clicking on a malicious link that would infect their device.



Phishing may take various forms. It was reported that Google and Facebook were duped out of nearly $120 million by someone who delivered phony contracts and invoices requesting payment. In perhaps the most famous case of phishing, the campaign manager for Hillary Clinton's presidential campaign was duped into clicking on a malicious link and entering his Google login. This made his whole Gmail inbox public.

How to Prevent Phishing!

- Training

The first and most critical step in maintaining email security is to train your workers on how to identify phishing emails and what to do if they come across one. This training should also be ongoing. Phishing attacks are continuously developing.

- Create a process.

Companies will often receive phishing emails.Phishing emails will be sent to your company. So someone will ultimately fall for one. If this occurs, your firm must have a procedure in place that everyone is aware of and understands. Employees who suspect they have been phished must know who to contact. Employees must know who to contact when they have been phished. You may lessen the impact of a phishing assault by acting quickly.

- Restriction on Public Information

If attackers do not know your employees' email addresses, they cannot target them. Non-essential contact information, like phone numbers or physical locations, should not be published on your website or in public directories. All this information may be used to assist attackers in planning an assault.

- Check your Emails Carefully

If your workers get an email from an unknown source, they should be cautious. Second, most phishing emails contain mistakes, strange syntax, or stilted phrasing. Finally, look at the "From" address to determine whether it is unusual. Employees should report suspicious emails.

- Be Cautious with Links & Attachments

Do not click on links or download attachments until you have verified the source and established the integrity of the link or attachment. Attachments are particularly hazardous because they may include malware, such as ransomware or spyware, which can infect the device or network.

- Do Not Download External Stuff Automatically

Remote content in emails, such as photographs, might execute unexpected scripts on your machine, and sophisticated hackers can hide harmful malware in them. You should instruct your email service provider not to download distant material automatically. This allows you to validate an email before running any unknown scripts included inside it.

- Never Communicate Critical Information Until You Know Who is on the Other End

NO ONE SHOULD EVER ASK FOR YOUR PASSWORD VIA EMAIL. This should raise a red flag if you get an email requesting you to give your password, credit card number, or other information.

- Hover Over Hyperlinks

Never click on hyperlinked text without first hovering your mouse over it to check the destination URL, which should appear in your window's lower right corner. A malicious link may sometimes be disguised as a short URL by the hacker. Using this programme, you may get the original URL.

- If In Doubt, Investigate It

Phishing emails frequently try to generate a false feeling of urgency by claiming that something demands quick action on your part. If your staff are unsure if an email is actual, they should not be hesitant to spend the extra time verifying it.

- Take Precautionary Measures

An end-to-end encrypted email service adds extra security to your company's communications during a data incident. A spam filter will filter out the various random emails you may get, making it more difficult for a phishing assault to succeed. Finally, other technologies, such as Domain-based Message Authentication, Reporting, and Conformance (DMARC), assist you in determining if an email originated from the person it claims to come from, making it simpler to spot possible phishing attempts.

What to do if your Comapny is Phished?

- Follow your company's procedures.
- Alert others, including customers, if necessary

Best Practices for Employee Email Security

- Know how to identify phishing emails
- Be aware of the dangers of email attachments
- Inspect links before clicking on them
- Disable the loading of remote content
- Think carefully before using "Reply All."
- If in doubt about an email, investigate further.
- If still in doubt, suspicious report emails to your IT security leader
- If you fall for a phishing scam, REPORT IT IMMEDIATELY

Conclusion

Why is Celayix so concerned about IT security? Celayix data security in our products and for our website visitors is vital to us. GDPR and the extension of new data privacy requirements remind us of our obligations to clients, employees, and website users. Similarly, at Celayix, our Cybersecurity policy is strictly implemented to protect data from breaches. Celayix strives to reduce as many security threats as possible while working with personal data or corporate equipment. The future of data security in modern business looks bright with a sensible cybersecurity policy!

References

https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-data-security/

https://blogs.oracle.com/oraclehcm/post/why-hr-data-management-and-security-is-safer-in-the-cloud

https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-from-home.html

https://www.zdnet.com/article/bad-news-the-cybersecurity-skills-crisis-is-about-to-get-even-worse/

https://blog.1password.com/state-of-access-report-burnout-breach/

https://gdpr.eu/what-is-gdpr/

https://www.proofpoint.com/us/threat-insight/post/proofpoint-releases-q4-2018-threat-report-and-year-review

https://www.ic3.gov/Media/Y2018/PSA180712

https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html