



Governance, Legislation and Ethics Work-Based Project

10th August 2020 - Siobhan Stephens

1800709 – University of Wales Trinity Saint David

Table of Contents

1	Assumptions	2
2	Report for the Attention of the Head of Information Governance	2
3	Report for the Executive Board	2
4	Discussion note for Governance Committee.....	2
5	Appendix A.....	4
6	Appendix B.....	16

1 Assumptions

The following assumptions have been made throughout the project:

- Company Name: ABC Technology
- Date of Incident: 8th July 2020
- Number of Staff Affected: 312
- Employee Name: Karen Jones
- Customer Name: William Perkins

2 Report for the Attention of the Head of Information Governance

Please see appendix A for report to Head of Information Governance.

3 Report for the Executive Board

Please see appendix B for report to Executive Board.

4 Discussion note for Governance Committee

Discussion Note - Governance Committee Meeting 13th July 2020

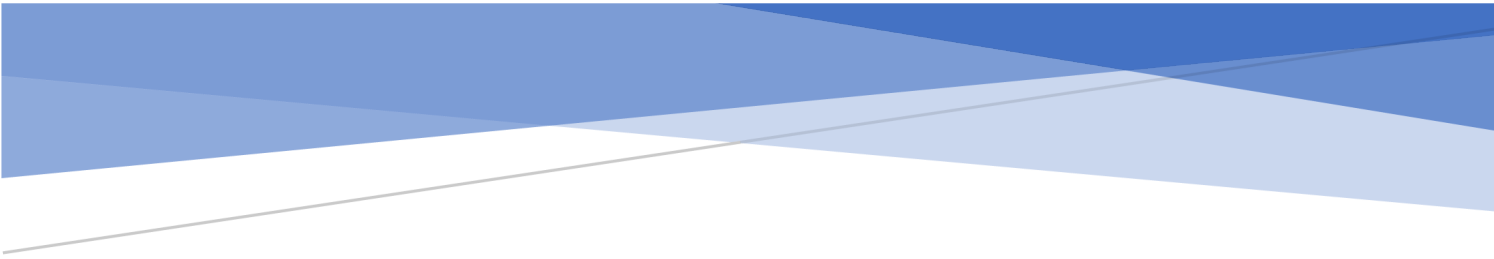
Possible approaches to minimise the likelihood of any future breach of this type:

- 1) All staff are to undertake refresher training on company policy and the importance of data security.
 - a. Training should fully cover GDPR principles and how to comply, along with the company's specific policies on data security, data storage, accountability and code of conduct.
 - b. A short GDPR and company policy based 'test' could be conducted at the end of training, to ensure the standard of training was sufficient and that staff members fully understood what was being taught. If a staff member was to fail, they should retake the training.
- 2) As mentioned above in section 3, further security surrounding email contents sent to external email addresses must be implemented to safeguard from employee mistake.
 - a. This could be implemented in various ways, such as only allowing emails being sent to external email addresses to contain files from certain server folders (eg customer sales leaflets) – this ensures other documents cannot be sent by mistake. This method would be cost-effective and would be quick to set up by the IT department and would suitable mitigate against a risk of this type in the future.
 - b. Further to this, complex scanning algorithms could be investigated, to check email body content for personal and sensitive data, however, this likely to be a slower ongoing process due to costs etc

- 3) Staff access rights should be investigated, as part of the ongoing company compliance policy, to ensure that only necessary staff have access to personal data.
 - a. Given that the staff member was an operational manager, it is understandable that they have limited access to the given staff information system, however, it should be investigated whether downloads should be allowed.
- 4) Further random checking and auditing of staff in line with company policy to be undertaken to ensure compliance with the company policy and code of conduct.
 - a. This should entail the steps covered in section 2.9 of the company policy document, including things such as ensuring staff do not share passwords or workstations, that paper documents containing personal information is not left unattended or not locked away, along with auditing that staff are following file organisation standards as set out in the company policy.

Appendix A

Report for the Attention of the Head of Information Governance.



ABC TECHNOLOGY SECURITY BREACH INCIDENT REPORT

For attention of the Head of Information
Governance, 10th July 2020

Information Governance Team

Abstract

This report outlines an incident which occurred on the 8th July 2020 at 2:32pm regarding an external security breach containing personal information about ABC Technology company staff, where an email was sent to a member of the public by an Operational department manager. It discusses the incident details, the breaches of the General Data Protection Regulation and company policy, the specific company policy surrounding this incident, and the actions to be taken as a result.

Table of Contents

1	Incident Details	3
2	Company Policy	3
3	Discussion	6
4	Actions	7
5	Consequences and Risks.....	8
6	Conclusion	9
7	Bibliography.....	10

1 Incident Details

On the 8th July 2020, a manager from the operational department, Mrs Karen Jones, alerted the information governance team of a security breach that occurred that day at 2:32pm, where they mistakenly attached a document containing personal information including names and addresses of 312 ABC Technology company staff on an email and sent this to a member of the public, Mr William Perkins. It was stated by Mrs Jones that she had downloaded the list from an operational system in order to increase efficiency of her role. Upon further investigation of Mrs Jones' work computer, the information governance team has discovered that scanned copies of staff sick notes and occupational reports have accumulated on the desktop.

As a result of this security breach regarding personal data, two of the General Data Protection Regulation principles have been breached. Firstly, the Integrity and Confidentiality (Security) principle.

Article 5(1)(f) of the GDPR concerns the 'integrity and confidentiality' of personal data. It says that personal data shall be: *'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'* [1].

Data has not been appropriately protected against accidental loss, as per this breach.

Secondly, the Accountability principle, or Article 5(2) of the GDPR says: *"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles]"* [2]. A security breach of this nature suggests that organisational policies and practices need to be reconsidered, and that frequent checking of compliance has not been adhered to, and therefore, is a breach of the above principle.

The following section outlines relevant company policy regarding these GDPR principles.

2 Company Policy

Below are abstracts taken from section 2.7 of the ABC Technology Information Governance & Data Security and Protection Policies document, version 3.4.1.

Ensure appropriate technical and organisational measures are in place, including:

- a) adopting and implementing data protection policies;
- b) written contracts between ourselves and organisations that process personal data on our behalf;
- c) maintaining strict documentation outlining our processing activities [2];
- d) recording and reporting personal data breaches internally, and, if applicable, to the ICO within 72 hours;

...

Section 2.10 of the document outlines company policy regarding the Integrity and Confidentiality of Data, along with mention of Accountability:

2.10.1 Data quality and reuse

Data quality must be of high standard and duplication must be avoided, along with inaccuracy and inconsistencies across personal information. We [ABC Technology] must maintain comprehensive records management policies per department to help avoid excessive retention or premature destruction of personal information. We will only use personal information where strictly necessary, and the use of anonymised data is preferred where possible [3].

2.10.2 Data Subjects' rights

We [ABC Technology] have a Records Management Policy to ensure that individuals can exercise rights over their own personal data in line with GDPR.

2.10.3 Data Security

Personal data should be kept secure at all times. We ensure that there are adequate policies and procedures in place to protect against unauthorised access, loss, destruction and damage [3], through the use of both physical and technological security.

2.10.4 File Storage and Organisation

Staff must follow the file organisation and storage policy as set out per department. This is to ensure security and confidentiality to each document, and to ensure only those authorised to access documents are able to. Under no circumstances should files be stored on desktops or in unsecured folders off of the company server. Files must only be stored for as long as necessary. In addition, paper records that have been entered into a system, such as the HR system, should either be safely stored using records management policy, or be destroyed.

2.10.5 Acceptable Use

Staff must use company computers for only their intended use, and not for any personal use, including during break times.

2.11.6 Responsibility

It is the responsibility of the staff member to ensure that company policy is complied with, and that the computer and any personal documentation is kept secure at all times. A failure to comply or take reasonable care may result in disciplinary or criminal actions against the employee, as set out in Section 3.1.

Section 2.9 of the document outlines company procedure regarding ensuring ongoing security and accountability compliance, an abstract of the applicable policies is below:

In order to ensure continual compliance with the GDPR , we must take the following steps:

a) Carry out frequent compliance checks, every 3 months, involving the following:

a.1) Physical Security Checks

- i) Ensure offices are locked when there are no members of staff present;
- ii) Ensure external media such as external drives are kept secure at all times;
- iii) Ensure computers are locked when the member of staff is not present, no computer should be left on and unattended;
- iv) Ensure that members of staff do not share workstations, or allow access to their workstation by another member of staff;
- v) Ensure that access to server and IT rooms is locked at all times, and that access is permitted only to the necessary members of staff;
- vi) Ensure that staff do not share passwords with others, or leave passwords visible, such as on a note on their desk;
- vii) Ensure that all paper documents containing personal information are not left unattended, and should be stored in a locked cabinet, or destroyed in a shredder when no longer required;
- viii) Ensure that no paper document containing personal information is to leave the office, or to be shared with another member of staff without prior permission from the department manager;
- ...

a.2) System Checks

- i) Ensure the proper file organisation structure is being adhered to, as per departmental policy, to maintain proper security and confidentiality to each file;
- ii) Ensure that passwords are being updated at least every 3 months as per the company password policy, and that passwords are of a secure type and adhere to company policy;
- iii) Audit system access rights for each role, with the 'least access' approach. Ensure that no member of staff has access to any system they do not require;
- iv) Continually audit accessed websites and ensure access is only permitted to reasonable addresses – others should be blocked;
- v) Ensure all downloaded resources are scanned for virus' on the server before downloading or opening;
- vi) Ensure that external media such as USB pen drives cannot be used, and are blocked;
- ...

b) Carry out frequent major compliance checks, every 6 months, involving the following:

...

b.2)

- i) Audit staff access rights to IT systems, and ensure staff have only the least required access, this includes their read, write and download access.
- ii) Audit staff desktops and file systems, to ensure proper storage policy is being followed, as per department policy.

c) Carry out training to educate all members of staff on the GDPR, company policy, and the steps on how to comply with all policies, every 12 months.

c.1) Staff must acknowledge training and compliance by signing a code of conduct document, stating their responsibility to ensuring data is kept safe.

Section 2.9.a.2.i discusses the 3 monthly checks to “Ensure the proper file organisation structure is being adhered to, as per departmental policy, to maintain proper security and confidentiality to each file”. However, it is apparent from investigation of Mrs Jones’ desktop, where multiple highly sensitive sick notes and occupational health reports were found to have accumulated, that these checks are not being sufficiently carried out across departments and members of staff. It is clear that an investigation into this policy and how it is undertaken must be done. The storage of such files by Mrs Jones’ in an unsecure manner is a breach of company policy, as per section 2.10.4, where it states “Under no circumstances should files be stored on desktops or in unsecured folders off of the company server”. As a result, section 3.1 of company policy, as stated below, outlines the actions that may be taken against an employee:

3.1 Breach of Company Policy

If it is found that an individual has either purposefully or accidentally not taken appropriate care to comply with company policy, ABC Technology has the right to take disciplinary measures against the employee. Further to this, if it is found that disciplinary measures are not suitable, ABC Technology has the right to terminate the employment contract after investigation. If necessary, criminal action may be taken against the employee.

Therefore, a separate investigation must be undertaken against Mrs Jones, and a discussion on disciplinary and/or termination action against her must be completed in due course.

Section 2.7.d states that security breaches must be reported internally and reported to the ICO if applicable. The ICO states that “A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of the risk to people’s rights and freedoms, following the breach. If it’s likely there will be a risk, then you must notify the ICO [4]”. It is felt by the Information Governance team that due to the fact that personal staff data was sent outside of the organisation to the member of the public, and this data contained both names and addresses, that the breach should be reported to ICO immediately.

As stated in the above policy extracts, it is clear the company takes care to ensure that GDPR is complied with. However, weaknesses in the current staff training and auditing process have been identified.

3 Discussion

The above company policy safeguards against many potential security breaches, however, this incident is an example of one it does not. ABC Technology places trust in its staff and

assumes that they will take reasonable care when sending emails and attachments to customers, but, in light of such an incident, a new policy must be implemented.

ABC Technology does not currently have any systems or policies in place regarding email attachments, which allows staff to upload and attach any file to an email – this is due to the company requirement of having to attach sales PDF's to customers, such as during this incident. There are two potential ways to protect against this, firstly that the necessary IT department research technology to allow for email and attachment scanning, so that personal details cannot be sent, or secondly, allow only documents uploaded to certain company folders, such as a 'Customer Information Leaflets' to be sent to external email addresses. This would mitigate against the current security incident and would not allow for mistakes such as these to occur.

Secondly is the issue of the manager, Mrs Jones, having accumulated scanned sick and occupational health notes on her desktop. This is severe misconduct and a breach of company policy, and as a result Mrs Jones' is must be placed under investigation, however, these documents should have raised concern during a 3 monthly compliance spot check, suggesting that these checks are not being carried out thoroughly enough. The information governance team is currently investigating the cause of this.

4 Actions

It is recommended by the Information Governance team that the following actions be made:

Immediate Actions

- 1) The customer affected, Mr William Perkins, must be contacted immediately and informed that he must destroy the email and file, if not already done so.
- 2) All 312 staff members whose details were breached must be contacted and informed, so that they are aware and can take precautionary measures to protect themselves if required.
 - a. This notification must contain a description of when and how the breach occurred and what data was involved. Along with outlining the steps the company has taken to mitigate risks [4].
- 3) All staff are to undertake refresher training on company policy and the importance of data security.
 - a. It is recommended that a basic test following staff training is to be undertaken, to ensure that staff have a full understanding of the company policy, their responsibilities and duties.
 - b. If an employee is to fail the test, they must undertake further training.
- 4) Further security surrounding email contents sent to external email addresses must be implemented to safeguard from employee mistake.
 - a. As mentioned in section 3 [discussion], this may be through the use of restricting file access for email attachments to specific folders, and/or through the use of email scanning algorithms.

- 5) The manager, Mrs Jones, must be investigated for misconduct as a result of incident, along with the extremely sensitive data held on her desktop without adequate security, breaching company policy and therefore code of conduct.
 - a. Disciplinary action may be taken against Mrs Jones as stated in the company policy section 3.1.

Ongoing Actions

- 6) Staff access rights to files, folders and systems should be investigated, as part of the ongoing company compliance policy, to ensure that only necessary staff have access to personal data.
- 7) Further random checking and auditing of staff to be undertaken to ensure compliance with company policy.
 - a. An investigation by the information governance team must be undertaken to understand the cause of why the documents were not discovered on Mrs Jones' desktop during the routine compliance checks.
 - b. Updates may need to be made to company policy surrounding these audits to make them more robust.

5 Consequences and Risks

The following consequences and risks are applicable as a result of this security breach, as identified by the information governance team.

Primary Consequences

- a) Potential fines and/or actions against ABC Technology
 - i) If in breach of eIDAS Regulation, ICO have the power to impose fines of £1,000
 - ii) ICO Audit. An audit may take place to ensure compliance and make recommendations where applicable
 - iii) ICO may serve an Enforcement Notice if there has been a breach, and provide recommendations on how to comply
 - iv) Prosecute if there is a failure to comply
 - v) If there is a failure to comply, there are also powers to impose fines of up to €20 million, or 4% of total worldwide annual turnover, whichever is higher.
- b) Disciplinary action or termination of contract of employee in question. Potential requirement to recruit new member of staff to undertake this role.

Secondary Consequences

- c) Loss of company trust and reputation from customers if the breach were to be publicly announced
- d) Loss of company trust and reputation from staff due to the loss of their data
- e) Loss of business due to the breach and tainted reputation
- f) Loss of share price and shareholders due to reputation
- g) Disciplinary/termination of contract for member of staff at fault, and any other staff found to be in breach of company policy and code of conduct
- h) Alterations to company policy, training and security measures to mitigate further risk

Risks

- a) Disgruntled employees due to the loss of their data
- b) Security breach could occur again if the actions mentioned above, such as effective training and security mechanisms are not put in place in a timely manner
- c) Other company policy/GDPR breaches may currently exist, such as those similar to Mrs Jones' unorganised and insecure desktop file organisation. A thorough investigation must be undertaken in due course to capture any other potential breaches and risks.

6 Conclusion

As highlighted in this report, the incident on 8th July 2020 where personal data containing names and addresses of 312 members of staff were sent to an external member of the public, is of high importance and has many consequences to ABC Technology.

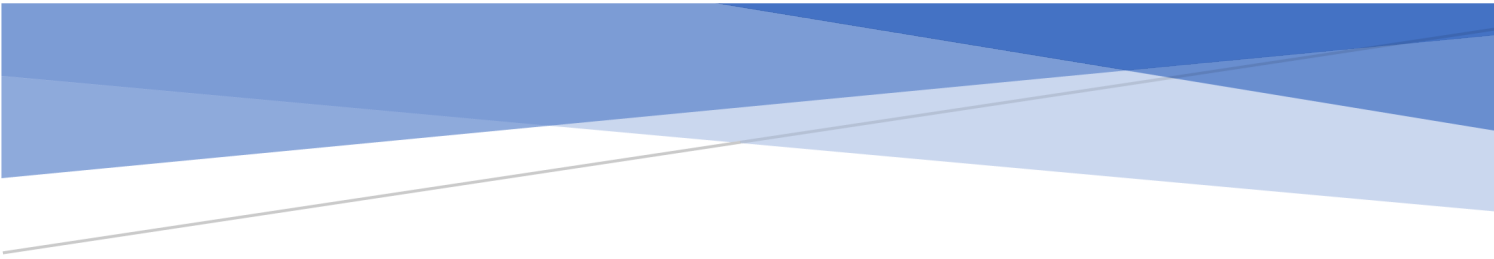
The actions contained within this report must be undertaken immediately in order to contain the situation and meet the ICO deadline of 72 hours to report a breach. If these actions are undertaken, the risk of another incident of this type will be mitigated and many of the potential risks can be contained, with benefit to the company.

7 Bibliography

- [1] "Security | ICO." <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/> (accessed Jul. 08, 2020).
- [2] "Accountability and governance | ICO." <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/> (accessed Sep. 08, 2020).
- [3] "Information Governance & Data Security and Protection Policies," 2018. Accessed: Sep. 10, 2020. [Online].
- [4] "Report a breach | ICO." <https://ico.org.uk/for-organisations/report-a-breach/> (accessed Jul. 08, 2020).

Appendix B

Report for the Executive Board.



ABC TECHNOLOGY SECURITY INCIDENT REPORT

For Attention of the Executive Board, 10th July 2020

Information Governance Team

Abstract

This report outlines an incident which occurred on the 8th July 2020 at 2:32pm regarding an external security breach containing personal information about ABC Technology company staff, where an email was sent to a member of the public by an Operational department manager. It discusses the incident details, the breaches of the General Data Protection Regulation and company policy, the specific company policy surrounding this incident, and the actions to be taken as a result.

Table of Contents

1	Incident Details	3
2	Actions	3
3	Consequences and Risks.....	4
4	Conclusion	5
5	Bibliography.....	6

1 Incident Details

On the 8th July, a manager from the operational department, Mrs Karen Jones, alerted the information governance team of a security incident that occurred that day at 2:32pm, where Mrs Jones mistakenly attached a document containing personal information including names and addresses of 312 ABC Technology company staff on an email and sent this to a member of the public, Mr William Perkins. It was stated by Mrs Jones that she had downloaded the list from an operational system in order to increase efficiency of her role. Upon further investigation of Mrs Jones' work computer, the information governance team has discovered that scanned copies of staff sick notes and occupational reports have accumulated on her desktop.

As a result of this security breach regarding personal data, two of the General Data Protection Regulation principles have been breached.

2 Actions

The ICO states that *"A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of the risk to people's rights and freedoms, following the breach. If it's likely there will be a risk, then you must notify the ICO [1]."*

During this incident, personal and identifying data pertaining to staff members were sent outside of the organisation to a member of the public. If this incident had occurred internally, such as to another member of staff, it would still be a breach of GDPR but would be more easily contained. However, it cannot be guaranteed that the member of public will rightfully and adequately destroy the email and file, and so, the rights and freedoms of the members of staff are at risk. Therefore, it is felt by the Information Governance team that due to the fact that personal staff data was sent outside of the organisation to the member of the public, and this data contained both names and addresses, that the incident should be reported to ICO immediately.

ICO and company policy regarding reporting the breach must be followed, including contacting the member of public affected immediately to request that they destroy the file and the containing email, and contacting every affected member of staff so that they can take necessary precautionary measures to protect themselves if required.

A further detailed list of actions to mitigate against further risks of this type, and disciplinary measures against the member of staff has been presented to the Head of Information Governance in a separate report.

3 Consequences and Risks

The following consequences and risks are applicable as a result of this security breach, as identified by the information governance team.

Primary Consequences

- a) Potential fines and/or actions against ABC Technology [2]
 - i) If in breach of eIDAS Regulation, ICO have the power to impose fines of £1,000
 - ii) ICO Audit. An audit may take place to ensure compliance and make recommendations where applicable
 - iii) ICO may serve an Enforcement Notice if there has been a breach, and provide recommendations on how to comply
 - iv) Prosecute if there is a failure to comply
 - v) If there is a failure to comply, there are also powers to impose fines of up to €20 million, or 4% of total worldwide annual turnover, whichever is higher.
- b) Disciplinary action or termination of contract of employee in question. Potential requirement to recruit new member of staff to undertake this role.

Secondary Consequences

- c) Loss of company trust and reputation from customers if the breach were to be publicly announced
 - i) A recent survey by Verizon discovered that 29 percent of customers said they would never use the brand again if they had compromised their information [3]
- d) Loss of company trust and reputation from staff due to the loss of their data
- e) Loss of business due to the breach and tainted reputation
- f) Loss of share price and shareholders due to reputation
- g) Disciplinary/termination of contract for any other staff found to be in breach of company policy and code of conduct
- h) Alterations to company policy, training and security measures to mitigate further risk

Risks

- a) Disgruntled employees due to the loss of their data
- b) Security breach could occur again if the actions mentioned above, such as effective training and security mechanisms are not put in place in a timely manner
- c) Other company policy/GDPR breaches may currently exist, such as those similar to Mrs Jones' unorganised and insecure desktop file organisation. A thorough investigation must be undertaken in due course to capture any other potential breaches and risks.

These risks are for the given external security incident, however, as previously stated, Mrs Jones was found to have scanned copies of sick notes and occupational health notes on her desktop. Names and addresses of staff are classed as personal information, but have little value in the majority of circumstances, therefore despite multiple risks and consequences, they are of a lesser nature than if sensitive data was to have been lost. The following are the potential risks if the sensitive health reports were to have been involved, in addition to the ones mentioned above.

- a) Blackmail against the company, for example to keep data private
- b) Blackmail against employees regarding the sensitive information
- c) Victimisation of members of staff, both inside and outside of the workplace
- d) Potential for compensatory costs to staff for loss of sensitive data

Therefore, it is clear that this additional potential GDPR breach must be investigated thoroughly with immediate effect. Actions to be taken regarding this and the employee in question have been advised to the Head of Information Governance in a separate report.

4 Conclusion

As highlighted in this report, the incident on 8th July 2020 where personal data containing names and addresses of 312 members of staff were sent to an external member of the public, is of high importance and has many consequences to ABC Technology.

The actions identified by the Information Governance team must be undertaken immediately in order to contain the situation and meet the company policy and ICO deadline of 72 hours to report a breach, and to mitigate against a further breach of this type.

Finally, whilst the data breach is both concerning and unfortunate, we can use the lessons learned to improve our systems, policies and practices to ensure both our staff and customer data is processed and stored safely. This should be a steppingstone for continued improvement within the company towards attaining a higher level of compliance.

5 Bibliography

- [1] "Report a breach | ICO." <https://ico.org.uk/for-organisations/report-a-breach/> (accessed Jul. 08, 2020).
- [2] "Enforcement | ICO." <https://ico.org.uk/for-organisations/guide-to-eidas/enforcement/> (accessed Aug. 08, 2020).
- [3] "What customer experience do consumers REALLY want? | About Verizon." <https://www.verizon.com/about/news/what-customer-experience-do-consumers-really-want> (accessed Sep. 11, 2020).