The MSP's Guide to Selling Backup

How to position backup, business continuity
and disaster recovery solutions to your clients

About this guide

This guide walks you through five steps to help your clients understand the importance of getting started with backup and business continuity solutions, then closes with advice and resources to help you sell.

Introduction

Painting the picture

Building your stack

Selling the solution

Introduction

There's a perception gap around the risk of data loss

You know that saying "you don't know what you've got 'til it's gone"? It can be hard to get SMEs to grasp just how valuable and vulnerable their data is until it's been compromised. You aren't the only MSP struggling to convey the urgency of backup and business continuity solutions to clients who have an "it won't happen to me" mindset.

As an MSP, you recognise the threats to data...

85% of organisations suffered at least one cyberattack in the preceding 12 months; an increase from 76% experienced in the prior year.[1]

... but most end clients aren't aware or prepared.

18% of SMEs believe they don't need an IT disaster recovery plan because they assume they would not be the target of a cyberattack.[2]

That's why it's important to start a conversation about backup and business continuity solutions by illustrating to your clients that the threat of data loss is real and can hurt their businesses. It's why the best time to sell an umbrella is when it's sunny out. Once it starts to rain, it's already too late.

Introduction

Remote work and cybercrime: the one-two punch

1. The rush to enable remote work

The continued surge in remote work left IT teams scrambling to enable remote productivity. Which has resulted in a broader surface area in security vulnerabilities due to employees:

- Working outside the safety of the corporate firewall
- Using multiple devices, including sometimes using personal devices for work
- Connecting via potentially unsecure home networks
- Allowing family members to use work devices

2. A flood of COVID-related cyberattacks

As of 2023, over 72 percent of businesses worldwide were affected by ransomware attacks.[3] Microsoft reported that pandemic-themed phishing and social engineering attacks jumped by 3,500 daily[4] in the UK alone, and ransomware attacks in Europe doubled in 2021.[5]

The result? Businesses were left bruised

The double whammy of a weakened security posture colliding with a flood of cyberattacks brought the consequences of data loss home to many companies.

24% of surveyed IT leaders said they paid unexpected costs to address a cyber breach or attack following the move to remote work.[6]

52% of MSPs reported that shifting client workloads to the cloud came with increased security vulnerabilities.[7]

Painting the picture

1. Start the conversation with stories and stats

Tell real-life stories and use research statistics to tangibly illustrate the cost of data loss and downtime. Below are a few real-life stories from the field and research statistics that make the cost of data loss and downtime tangible. This can help drive home to your clients why backup and business continuity solutions are necessary, even for SMEs.

Pharmaceutical company Reckitt Benckiser lost £107 million/€125 million in disrupted production, goods, clean-up, and recovery costs after being targeted by the NotPetya ransomware.[4]

A ransomware attack in February 2021 knocked two UK government services offline while investigators inspected the damage and took steps to mitigate further upheaval.[7]

Hackers attempted to extort money from multiple UK Voice Over Internet Protocol (VoIP) providers in October 2021 with an unprecedented and coordinated DDoS attack.[5]

In the UK, 44% of consumers will stop business with a breached entity for several months, and 41% will never return.[8]

Every minute of downtime costs an SME around £342/€400.[6]

2017's WannaCry ransomware attack cost the NHS £92 million/€107 million according to a government report.[6]

Other MSP anecdotes about data loss causes:

"overheated server closet"

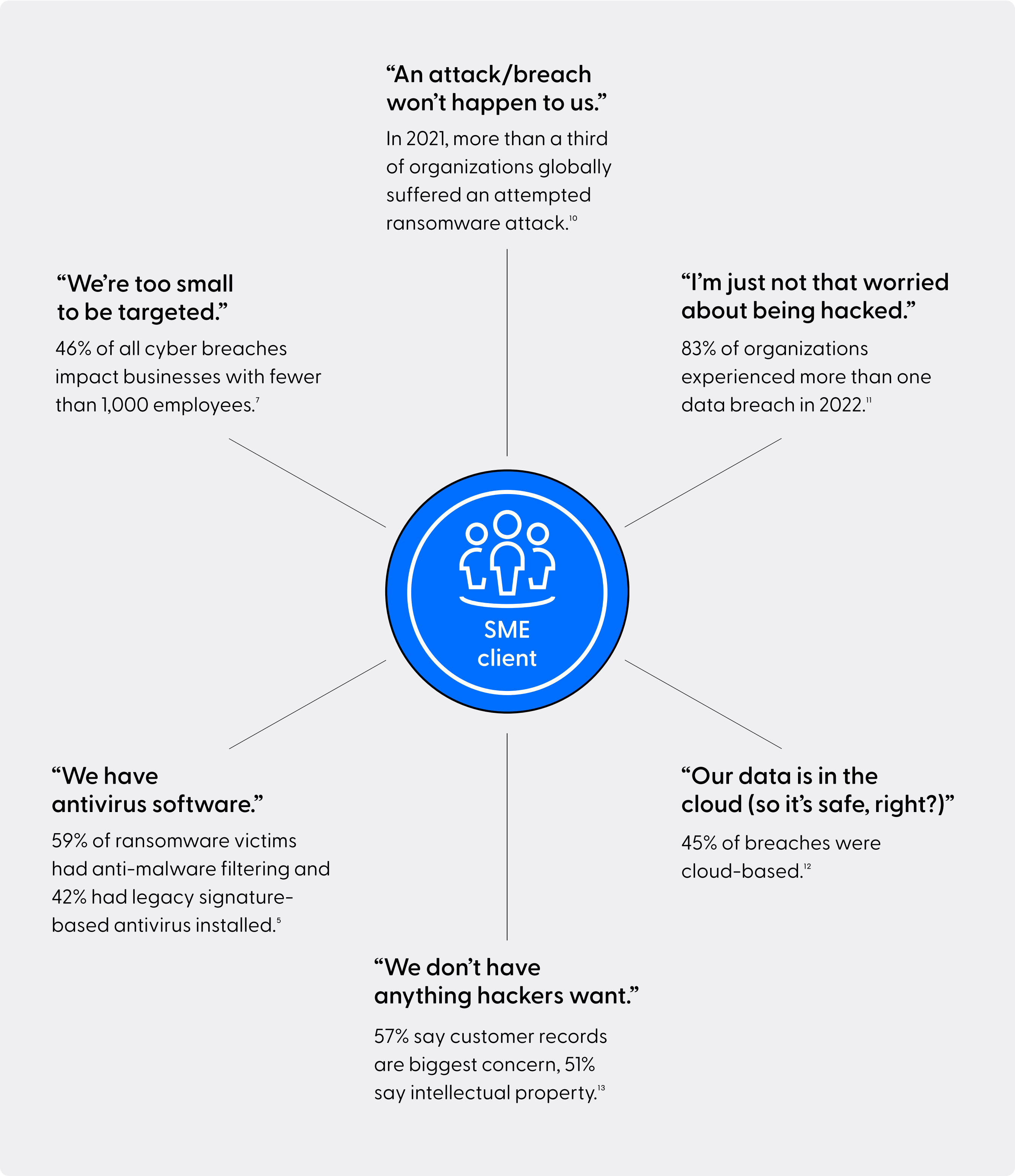
"actual fire inside a server"

"power surge during a storm"

"cat knocked external hard drive off a shelf"

Painting the picture

2. Overcome objections



SME client

"An attack/breach won't happen to us."

In 2021, more than a third of organizations globally suffered an attempted ransomware attack.[10]

"We're too small to be targeted."

46% of all cyber breaches impact businesses with fewer than 1,000 employees.[7]

"I'm just not that worried about being hacked."

83% of organizations experienced more than one data breach in 2022.[11]

"We have antivirus software."

59% of ransomware victims had anti-malware filtering and 42% had legacy signature-based antivirus installed.[5]

"Our data is in the cloud (so it's safe, right?)"

45% of breaches were cloud-based.[12]

"We don't have anything hackers want."

57% say customer records are biggest concern, 51% say intellectual property.[13]

Painting the picture

3. Explain the vulnerability of their data

Businesses of all sizes are under siege from an increasing volume and variety of cyberattacks. On top of malicious threats, there's also a wide range of accidental or uncontrollable ways your data can be lost or damaged. With so many possible risks to business data, it's clear that backup isn't optional any more.

User error

From accidental file deletion to overwriting to spilling coffee on laptops, user error is the primary cause of data loss.

Ransomware attacks

Even if you pay a ransom, you're not guaranteed to get all of your data back.

Other cyberattacks or breaches

From phishing to password attacks, network intrusions and malware, there's a variety of ways in which bad actors try to gain access to or corrupt valuable data.

Malicious deletion

There's a risk of angry employees on the verge of quitting or being fired purposefully deleting critical data out of spite or to cover their tracks.

Employee turnover

Well-meaning departing employees sometimes try to "clean" their devices and file systems before leaving.

Hardware failure

Hardware failures such as device or server crashes can lead to huge amounts of data loss.

Device loss or theft

Mobile workforces increase the risk of lost or stolen laptops and smartphones that contain corporate data.

Physical disasters and power outages

Fires and floods can destroy devices and servers, while power outages lead to data loss due to unsaved data or data corrupted by improper shutdowns.

Painting the picture

4. Explain the value of their data

A small business might think they don’t have any data of value, but the truth is, any customer or employee data can have value to the right person. Personally Identifiable Information (PII) can fetch a large price on the black market, and of course, competitors will always be interested in learning sales, financial and proprietary info.

Data’s resale value doesn’t matter when it comes to ransomware

Ransomware attackers don’t need to be able to monetise stolen data, they just need the victimised business to need their data back enough to pay up.

How much is business data worth to bad actors?*

Credit card info	£1.50 – £4/ €1.80 – €4.50 (per record)
Customer PII	£15 – £360/ €18 – €420 (per record)
Employee PII	£15 – £360/ €18 – €420 (per record)
Medical records	£15 – £40/ €18 – €45 (per record)
Sales/financial info	Competitive value
Proprietary info	Competitive value

* Estimated data values from The Sociable

Painting the picture

5. Cover industry-specific talk tracks

It's important to customise your backup/business continuity to any data protection needs specific to your client's industry. Here are a few talking points related to specific industries you can use to tailor your conversation.

Healthcare	**Top Target** Healthcare is reported to be the most vulnerable industry in 2023.[15]	**Compliance fines** Healthcare organisations face hefty fines and penalties for data protection breaches (fines can be in the millions).	**Lives are at stake** Ransomware attacks have crippled hospital patient care systems.
Financial	**Vulnerable industry** Businesses in the financial industry experienced a 1,318% year-on-year increase in ransomware attacks.[16]	**#2 target** The finance industry had the second highest average cost per breach, trailing only health care.[12]	**Drop in share performance** Finance and payment companies saw the largest drop in share performance.
Retail and hospitality	**Lost sales** 66% of retailers paid the ransom after a ransomware attack due to the threat of lost sales.[18]	**Vulnerable point of sale info** Most valuable info from hospitality businesses includes client information, passport information and credit card numbers.	

Painting the picture

5. Cover industry-specific talk tracks

State and local government	**Increasingly targeted** The rate of ransomware attacks in state and local government has increased from 58% to 69% year over year.[19]	**Ransom payments can be in the millions** UK councils are increasingly at risk from a ransomware attack.[9]	
Legal	**Not technical or prepared** 22% of law firms did not have an organised plan in place to prepare for, prevent or respond to data breaches.[20]	**Supply chain consequences** Food conglomerate, Mondelez, reported that the personal data of 51,000 of its current and former employees was compromised following a cyberattack on its law firm.[21]	**Potential for ethical violations** The potential for an ethical breach occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion.

Building your stack

Solution definitions and comparison

	Backup and SaaS backup	Business continuity (BC)/ Disaster recovery (DR)	High availability
Overview	Provides a system for the backup, storage and recovery of digital files and folders. Typically collects, compresses, encrypts and transfers the data to the remote backup service provider's servers or off-site hardware on a recurring or continual basis. SaaS backup can back up cloud apps (e.g. M365, G Suite, SharePoint, etc.).	Hardware appliance that lives on-site to back up data, which is also backed up to the cloud in a remote location to reduce downtime and data loss.	Often heavily intertwined with BC/DR solutions. Provides resource availability in a computer system in the wake of component failures that disrupt access to data resources and critical business applications. Usually encompasses functionality such as virtualisation and guaranteed recovery time windows.
Strengths	· Good entry-level point to start clients with backup · Affordable · No maintenance – files are backed up to the cloud automatically and regularly · Supports compliance · Reduces risk of data loss and mitigates potential damage from ransomware attacks	· Gets business back online after outages · Helps drastically eliminate downtime and data loss · Minimizes the interruption of critical processes · Mitigates potential damage from ransomware attacks and malware attacks · Supports compliance	· Protection from downtime · Real-time replication for more comprehensive protection than snapshots · Efficient, affordable remote data protection for off-site or total disaster recovery · Uses bandwidth-efficient replication to minimise the cost of remote data replication
Limitations	· Can take a long time to fully restore data	· Can be costly, depending on the type of BC/DR solution it can still take a while to restore data	· Can be costly, has more functionality than a lot of smaller businesses will need

Building your stack

Solution definitions and comparison

	Backup and SaaS backup	Business continuity (BC)/ Disaster recovery (DR)	High availability
Best for	· Cloud backup is often used to back up laptops, desktops, and servers · SaaS backup is used for protecting M365 clients, G Suite clients and SMEs	· Clients with critical applications that need to be accessible within minutes or hours · Clients in high-risk geo-locations (e.g., Southeast coast at risk of hurricanes), clients in compliance industries	· Clients whose business cannot tolerate any downtime or loss of access to critical data/apps
Discovery questions	How much data do you back up? How often do you conduct backups? How long do your backups take to complete? What would be the impact if a backup or recovery failed?	Do you need to comply with industry regulations for data protection? Have you experienced ransomware attacks or are you worried about the threat? Have you ever had a failed recovery from an outage or disaster situation?	If you lost or couldn't access critical data, would you be out of business?

Building your stack

Blending solutions to find the right coverage

It's imperative that clients protect their data and can quickly access that data when needed. Pax8 has best-in-class backup, business continuity, disaster recovery and storage solutions from top vendors that you can layer and blend to find the right data protection coverage for your stack.

Finding the best fit for continuity solutions depends on a wide range of unique factors, such as:

- Downtime tolerance
- Backup frequency needs
- Data volumes
- Scalability
- Reporting capabilities
- Budget

Selling the solution

MSP advice

“Because Microsoft says so”

It can be eye-opening for Microsoft clients to learn that Microsoft themselves recommend third-party backup solutions. The Service Availability section of the Microsoft Services Agreement states:

> *“We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your content or data that you’ve stored.* **We recommend that you regularly backup your content and data that you store on the services or store using third-party apps and services.”**

“… and the NIST Cybersecurity Framework agrees!”

As a gold standard of guidelines and best practices for managing and reducing cyber risk, the NIST Cybersecurity Framework is another great tool to demonstrate the critical importance of backup to your clients. Step five of the NIST Cybersecurity Framework is “recover” and includes backing up important data/info and scheduling incremental backups to make recovery from a data loss incident much less impactful.

Two powerful statistics to pull out of your back pocket

97% of organisations that had data encrypted got data back.

70% of those organisations used backup to do so.[9]

Selling the solution

MSP advice

Determine downtime tolerance

To identify the most appropriate business continuity solution for a client, it's important to establish their Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to understand to what extent downtime and data loss affects their business operations.

- **RTO** is *how long* a business can tolerate downtime before facing consequences (such as lost sales, angry customers, frustrated employees, etc.)
- **RPO** is *how much* data a business can tolerate losing (measured in units of time back to the most recent backup. E.g. if you backup hourly, your business would only lose an hour of data)

Establishing a client's RTO and RPO can help you determine whether they need a light or intense backup solution (or BC/DR and high-availability solutions with failover capabilities). Finding the right fit means that clients don't pay for more functionality and capabilities than they need.

Focus on the bigger security picture

In today's aggressive and sophisticated cyberthreat landscape, cyber resilience should be the ultimate goal for all business IT strategies. No security tool is 100% foolproof. Backup should be the last line of defence of a multi-layered security approach so that when a breach does happen, your clients can quickly recover their data and keep business going.

The continuity conversation should be about more than just "you should back up your Microsoft files". Continuity should be presented as a critical component of a holistic cyber-resilience strategy that layers on tools and solutions to cover as many bases as possible, especially during an era of remote work.

Selling the solution

MSP advice

Take a page out of insurance companies' books

Present backup and continuity solutions along the lines of an insurance expense. Businesses purchase insurance for their building, employee health and workers' compensation – continuity is like insurance for their data. The monthly cost of these solutions is a tiny expense compared to the potentially catastrophic cost of data loss, lost productivity and lost revenue due to downtime, ransomware payments and compliance fines.

Build their business continuity solution stack over time

Don't overwhelm clients by trying to set them up with full BC/DR capabilities at the start. The easiest first step for an SME to take to protect their data is to implement a third-party online backup solution that replicates data offsite in the cloud. As their business matures, you can then naturally progress to more complex and costly BC/DR and high-availability solutions if needed. The important thing is that your clients need to start somewhere to protect their data, so getting them covered by a cloud backup solution is a great first step.

Don't forget to lead by example

Last but not least, it's important that your MSP business has backup as well! Not only is it critical to protect your business and client data, but to be a trusted advisor, you need to demonstrate that you practice what you preach. Additionally, using the backup and BC/DR solutions that you sell will give you authority to speak to their value and benefits with first-hand experience.

Selling the solution

Sample email templates

While Pax8 doesn't recommend blasting your entire client base, we do recommend sending an email to a targeted list of your clients who are a good fit for a backup solution. Below is one of the multiple sample sales email templates we've written that you can customise for use with your clients, which you can download in the resources section at the end of this guide. And as always, feel free to reach out to Pax8 for assistance.

New email

To: **[Client email]**

Subject: **[Email Subject]**

Dear **[Client Contact First Name]**,

Did you know that Microsoft only keeps backups of your data for 30 days? If your emails or files are deliberately or accidentally deleted, but you don't realise until several weeks later, you won't be able to restore your data.

In fact, in the Microsoft Services Agreement, they recommend using third-party backup services.

That's why, to protect your data, we recommend adding **[INSERT BACKUP SOLUTION NAME]** to your solution set, as it provides:

- **[INSERT SOLUTION FEATURE, e.g., "[X]-times daily backups of Exchange Online, SharePoint, OneDrive, Office 365 Groups, and Microsoft Teams"]**
- **[INSERT SOLUTION FEATURE, e.g., "Multiple bulk and individual restore options"]**
- **[INSERT SOLUTION FEATURE, e.g., "Highly automated migration services"]**

In today's digital economy, adding a backup layer is no longer an option if businesses want to truly keep their valuable data safe.

I'm happy to set up a call to discuss this with you and answer any questions.

We appreciate your business and strongly recommend taking this step to protect your cloud data.

Thanks,
[Signature]

Selling the solution

Sample liability waiver templates

If, after you've explained all of the reasons that you strongly recommend backup, you still have a client that refuses to pay for a backup solution, you should consider protecting yourself by requesting they sign a waiver in which they acknowledge that they are declining backup coverage against your advice. Sending this waiver can also be a wake-up call for stubborn clients to realise how critical backup coverage is to protect against data loss. Below is a sample backup coverage liability waiver.

Please note: *This is a SAMPLE waiver only. Pax8 is not responsible for ensuring the legality or accuracy of the language in the text below. Always run any legal documents such as a waiver past your legal team for approval before distributing.*

Voluntary Waiver of Backup Coverage

Date: ______________________________
Client: _____________________________
Reseller X Advisor: ____________________

This form is notice that the Client hereby acknowledges that they were informed by their Reseller X Advisor about the potential need for and availability of cloud backup coverage. By way of signing this document, the Client hereby acknowledges that they have made the decision to waive their right to purchase cloud backup coverage at this time.

The Client also acknowledges that this is against the advice of their Reseller X Advisor and that by signing this document they are releasing any liability of the Reseller X Advisor by any and all parties who have or may have right to bring claim against any party with regard of the Client's decision to voluntarily decline cloud backup coverage.

The Client fully acknowledges that they have reviewed this document and they understand the effect of declining cloud backup coverage against the recommendation of the Client's Reseller X Advisor.

The Client understands that if they add cloud backup coverage at a later date, the price and options for coverage may change for a variety of reasons.

Client Signature: ____________ Date: ________ Reseller X Advisor Signature: _________ Date: ________

Client Name (Printed): ______________________ Reseller X Advisor(Printed): ________________________

Putting it all together

It is absolutely vital that your clients have business continuity in place. However, we know that many SMEs don't quite get that having backup is just as important as having cybersecurity. Pax8 is here to help you have those conversations with your clients and build the continuity stack that's best for you and your clients.

Other resources

Download:

- Sales email templates and sample liability waiver
- White-labeled fact sheet

Read:

Pax8 Continuity blog

Calculate:

Pax8 Downtime Cost Calculator

Learn:

Continuity Fundamentals course

Sources

1. '2023 Global Report Ransomware Trends', *VEEAM*, 2023, https://www.veeam.com/ransomware-trends-report-2023

2. 'Cyber-resilience during a crisis', *Kaspersky*, 2022, https://www.kaspersky.com/blog/smb-cyber-resilience-report-2022

3. 'Annual share of organisations affected by ransomware attacks worldwide from 2018 to 2023', *Statista*, 30 August 2023, https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

4. 'Exploiting a crisis: How cybercriminals behaved during the outbreak', *Microsoft Threat Intelligence*, 16 June 2020, https://www.microsoft.com/en-us/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/

5. 'ENISA Threat Landscape 2021', *Enisa*, October 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport

6. 'Enduring from home', *Malwarebytes*, 2020, https://www.malwarebytes.com/resources/files/2020/08/malwarebytes_enduringfromhome_report_final.pdf

7. 'Datto's Global State of the Channel Ransomware Report', *Datto*, 2020, https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf

8. 'Incident management for high-velocity teams', *Atlassian*, https://www.atlassian.com/incident-management/kpis/cost-of-downtime#

9. 'Data Breach Investigations Report', *Verizon*, 2021, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

10. 'Momentive study: Americans shrug at Russia cybersecurity risks', *Momentive*, April 2022, https://www.momentive.ai/en/blog/momentive-study-russia-cybersecurity-risks/

11. 'The State of Ransomware 2023', *Sophos*, May 2023, https://www.sophos.com/en-us/content/state-of-ransomware

12. 'The Latest 2023 Ransomware Statistics', *AAG*, September 2023, https://aag-it.com/the-latest-ransomware-statistics/

13. 'Cost of a Data Breach Report 2023', *IBM*, 2023, https://www.ibm.com/reports/data-breach

14. 'Cost of a Data Breach Report, 2022', *IBM*, 2022, https://www.ibm.com/reports/data-breach

15. '2018 State of SMB Cybersecurity Report', *Ponemon Institute*, 14 November 2018, https://www.ponemon.org/news-updates/news-press-releases/news/2018-state-of-smb-cybersecurity-report.html

16. 'The many motives of hackers and how much your data is worth to them', *The Sociable*, 1 July 2019, https://sociable.co/web/the-many-motives-of-hackers-and-how-much-your-data-is-worth-to-them

17. '2023 State of Ransomware', *Malwarebytes*, 2023, https://try.malwarebytes.com/business-2023-state-of-ransomware/

18. 'How Data Breaches Impact the Financial Industry', *Hartman Advisors*, March 2021, https://hartmanadvisors.com/how-data-breaches-impact-financial-industry

19. 'How data breaches affect stock market share prices', *Comparitech*, 9 February 2021, https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/

20. 'The State of Ransomware in State and Local Government 2023', *Sophos*, 1 August 2023, https://news.sophos.com/en-us/2023/08/01/the-state-of-ransomware-in-state-and-local-government-2023

21. 'Mondelēz retirement data breached after hacker targets law firm Bryan Cave', *Cybersecurity dive*, 21 June 2023, https://www.cybersecuritydive.com/news/mondelez-retirement-hacker-targets-law-firm/653600/