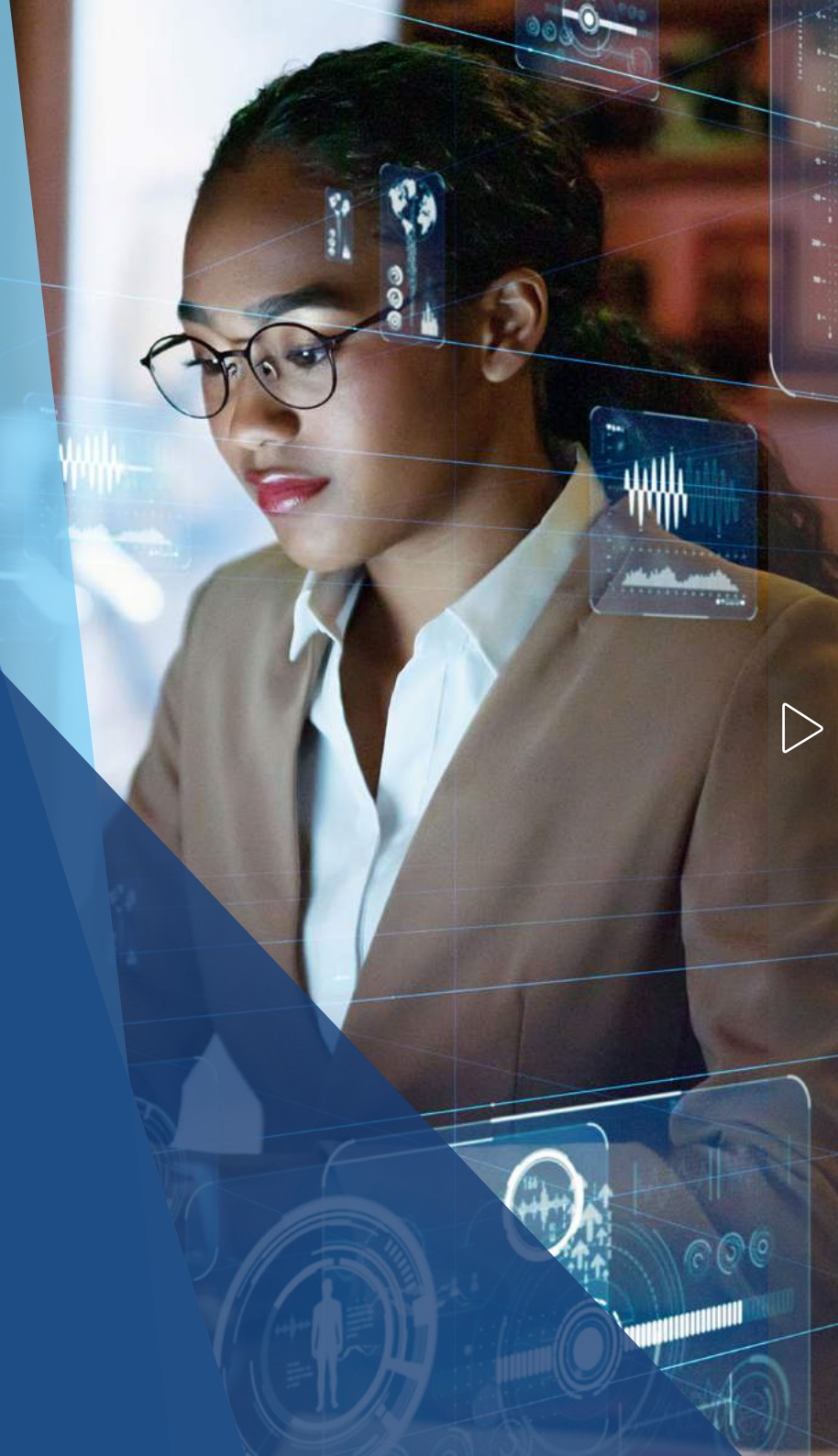
RETHINK YOUR BUSINESS

BEST PRACTICES IN CYBERSECURITY



IRON MOUNTAIN®

BEST PRACTICES IN CYBERSECURITY

Although the number of reported data breaches is down on last year, the cost of remediation continues to rise, as recent figures demonstrate:

- There were **3,932 publicly reported data breaches in 2020**[1], a 48% decrease from the previous year. That said, breaches that happened in 2020 continue to be reported in 2021.
- The **average cost** of a data breach reached an estimated at $4.23m[2] in 2020, up 10% over the previous year.
- **Healthcare was the most targeted** sector in 2020, accounting for 12.3% of all reported data breaches.[1]

The risk to businesses is not just the size of the fines. Class actions, falling share prices, loss of customer confidence, and reputational damage all have a significant impact on brands.

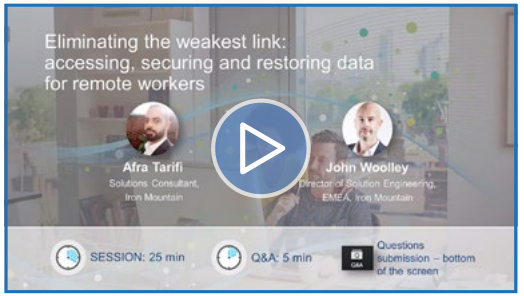
There are many tools that businesses can deploy in an attempt to ward off attacks. In this guide, we consider the bigger picture. How can you **implement cybersecurity best practices** throughout your organisation to protect the confidentiality, integrity and availability of your information systems – and recover in the event of a breach?

The impact of the pandemic has seen the rise of new threats and old ones with new variants, many of which specifically target those working from home. To mitigate these threats, IT leaders need to think outside the box and focus on measures like account-based security and role-based access.

DOES EVERY SIZE OF BUSINESS NEED TO WORRY ABOUT CYBERSECURITY?

Attackers are no respecters of size. While they may find the volume of customer data held by large organisations tempting, there is still much to be gained in accessing the supply and payment systems in smaller businesses.

In some ways the problem is even greater for small and medium-sized businesses. They have tight budgets for security measures, but cannot afford to be offline for any length of time. Attackers often see them as easy targets.



1. Hiscox/Risk based security: 2020 Year End Data Breach QuickView Report
2. IBM Security: 2021 Cost of a Data Breach

WHAT IS OUT THERE?

UNDERSTAND THE THREAT LANDSCAPE

Do you know what sort of attacks are possible and how they can affect your business?

- Statistics report that **malware** – malicious software – continues to be the greatest threat that we have to deal with every day. Computer viruses, worms, Trojan horses and spyware are all forms of malware. Simply clicking on an innocent-looking link can be enough to allow malware into your computer systems.

- **Double extortion ransomware** and **cryptojacking malware** are among the most common forms of malware. Ransomware actors are now more likely to exfiltrate sensitive data before they encrypt it, and threaten to release it onto the dark web if the victim fails to pay a ransom. While not as severe, cryptojacking malware is another growing threat, in which attackers hijack computing systems to mine cryptocurrency for them.

- **Phishing schemes** are focused on users, enticing them with credible-looking emails to give up personal and financial details. Phishing attacks are increasingly targeted, with two thirds of organisations reporting targeted phishing attempts in 2020[3].

There are many other types of attack launched by a wide range of players, from nation states through organised crime to hacktivists. With a ready market for almost all types of data, the shape, scale, and sophistication of cyberattacks continues to evolve at a rapid pace.

Experts in the field generally agree. It is not a matter of planning for whether or not your data is breached, but when it will happen. Developing a strategy to prevent attacks is imperative for businesses of all sizes.

3. 2021 State of the Phish, by Proofpoint

WHAT YOU CAN DO?

UNDERSTAND THE DATA THAT YOU HAVE

Do you know what data you have, and why you have it? Are you putting data that you should not even be holding at risk?

Understanding your data is an important first step. **Managing and protecting** data effectively and in compliance with the law is vital. That means employing good data governance, understanding how your data flows through the organisation, and securing it at every stage of the lifecycle.

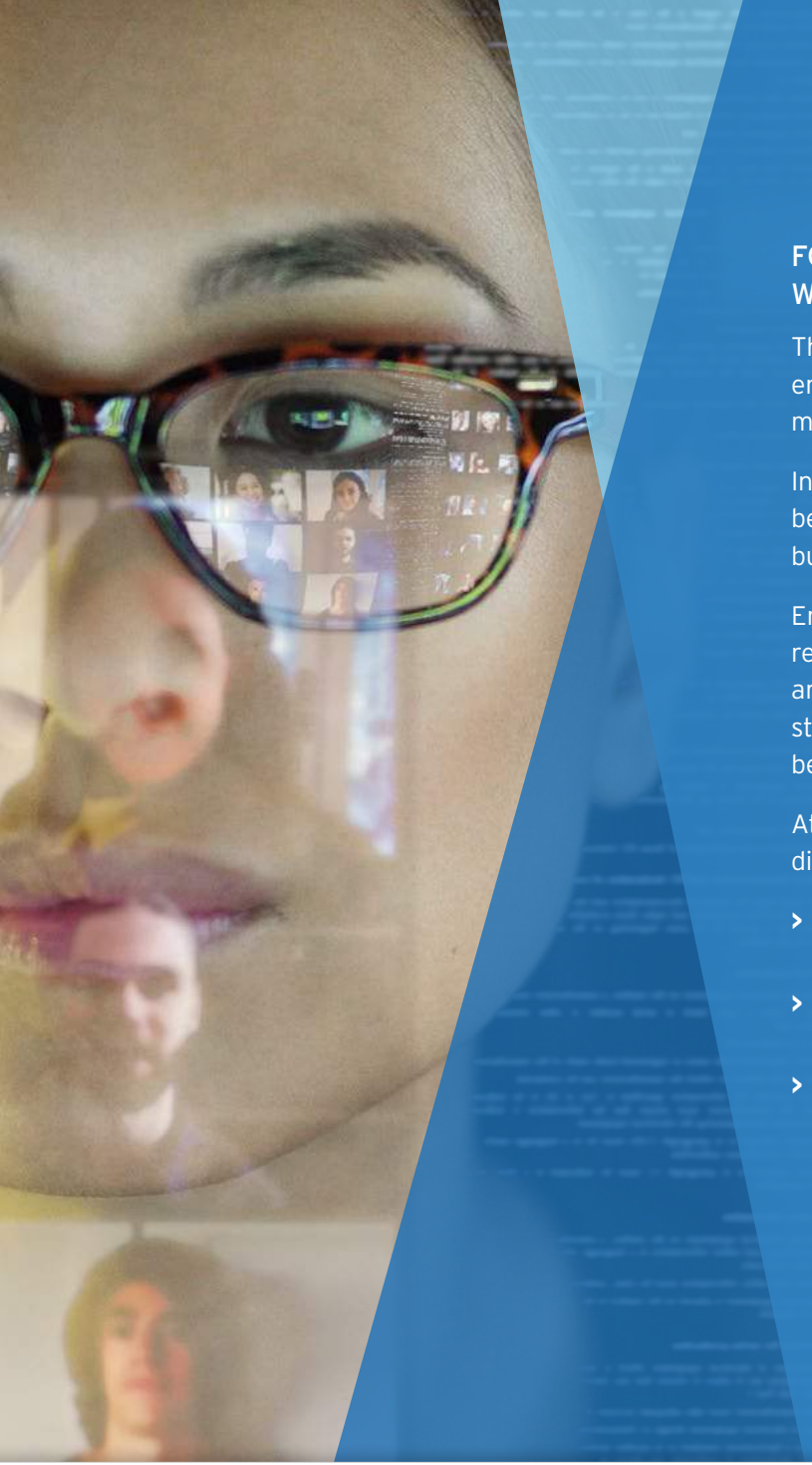
CREATE A RISK-BASED STRATEGY

The three primary risks that need to be managed are **business operational risk**, **reputational risk** and **legal and compliance risk**. While there is no one-size-fits-all approach to cyber risk management, there is great value in aligning with an established cybersecurity framework, such as ISO 27001 or the US National Institute of Standards (NIST).

It is worth talking to your insurer about which framework would best suit your particular situation.

TAKE THE WHOLE BUSINESS PERSPECTIVE

Cybersecurity is not just about technology. It brings together IT, legal, and security expertise to create a framework and challenge threats. And it is about every individual in the organisation being aware of how easy it is to become a target.



FOSTER A SECURITY-AWARE WORKING CULTURE

The human element is critical in creating a secure environment, especially with the rise of hybrid working models.

Insider threat, for example, is not always about people being malicious, but an innocent click on the wrong button that can allow a bad actor to enter the system.

Employees need to appreciate the risk and their responsibilities, and security awareness and training are key here. Deliver training that is appropriate to the stakeholder, explaining the importance of consistent behaviours and adherence to policies.

At the same time, it is necessary to address the issue of disgruntled employees or ex-employees by:

- **monitoring behaviour** and paying attention to apparent discontent
- **implementing processes** to assess and remove at-risk employees
- implementing role-based **access permissions**, and limit access to the most critical systems and data. Organisations should ideally follow a **zero-trust security** model and the **principle of least privilege** to ensure that access is always verified and people and devices only ever have access to the data they need to perform their roles.

DEVELOP STRONG GOVERNANCE

For your strategy to be successful, your organisation needs strong **governance and leadership**. This will enable the whole business to **align with cybersecurity** strategies, reduce the impact of breaches and enable better allocation and management of security resources.

A strong governance framework encompasses:

- senior leadership buy-in
- one person assigned with clear responsibility for cybersecurity leadership
- clear policies and procedures
- a strong cybersecurity culture
- an incident response and remediation plan

BUILD DEFENCE IN DEPTH

Protective controls can be breached, so it is important to deploy a **defence in depth** strategy to protect your assets, from the perimeter of your data right through each and every endpoint. If the attacker gets through one line of defence, you then have other lines of defence deployed.

Physical security, for example, should prevent people from unauthorised access. **Endpoint protection** should encompass physical, technical, and administrative safeguards.

At the same time, traditional measures, such as network and system controls, firewalls, intrusion prevention and access control measures, should be deployed alongside advanced threat protection tools.

FACTOR IN YOUR REMOTE WORKFORCES

Facing social-distancing and stay-at-home mandates, many organisations faced a sudden and urgent need to shift towards remote work models in 2020. But even as people return to the office, remote work is now well-established as the new normal.

Yet remote work presents unique cybersecurity concerns, with around 20% of organisations[4] having experienced data breaches due to remote workers. To mitigate these threats, organisations must:

- Implement tough endpoint security, such as encryption and physical measures
- Be wary of the unique risks presented by employee-owned devices
- Focus on account-based security and multifactor authentication
- Educate employees on the threats they face when working away from the office
- Govern data according to the data-retention rules of legislation like GDPR.

READ MORE ▷

4. https://blog.malwarebytes.com/reports/2020/08/20-percent-of-organizations-experienced-breach-due-to-remote-worker-labs-report-reveals/

DISASTER RECOVERY:
PLAN FOR THE WORST THAT CAN HAPPEN

Many businesses have **disaster recovery and business continuity plans**, but historically, they are about preparing for unexpected physical occurrences, such as a flood or fire. But cyberattacks that take the business down are just as disastrous, if not more so.

Consider the range of impacts that a successful attack could have on your business, and plan to manage that.

Questions to ask your business include:

- How long can your business survive an outage, and what are the critical applications that need to be restored as quickly as possible? Smaller businesses are more susceptible if the attack affects cash flow. Foundational infrastructure, upon which all your other systems run, requires especially close attention.
- How much are you willing to spend to survive an event? Storing data across multiple nodes, for example, might be more expensive, but also more effective.
- Are you considering every aspect of redundancy in your physical set-up, right down to the fibre that delivers connectivity in and out of the data centre?
- Are you training your staff in the event of a cyberattack, testing your disaster recovery programmes on a regular basis, and including your suppliers and partners in those drills?

A formal response plan makes it easier to deal with and recover from an attack. The fact is that attacks will happen, but what matters is how you discover and mitigate those attacks before they have far-reaching consequences.

In practical terms this means putting together an incident response team and training them continually. Rehearse the plan, conduct table-top exercises, and plan how to minimise human error. It can be a good idea to **engage a professional** incident response firm and place them on retainer with an SLA before any incidents occur.

- Develop a crisis-management plan that addresses both internal and external stakeholders to deliver on the plan and maintain confidence and trust.
- Plan for the contingency that normal communications may not be functioning during an incident.
- Finally, make sure that you have recent and comprehensive data backups.

WATCH OUR VIDEO ABOUT BUILDING A DISASTER RECOVERY PLAN

BUILDING YOUR DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN?

READ MORE ▷

ACT FAST IF THERE IS A BREACH

The average time to detect and respond to a breach Is 207 days, and it takes another 73 days on average to respond to it[6]. As such, the total average lifecycle of a data breach is 280 days.

The faster you can move, the lower the impact and cost. Companies that contain a breach in less than 30 days have reportedly saved over a million dollars.

DISCLOSE A BREACH AS EARLY AS YOU CAN

When, in spite all your planning, you experience a data breach, declare it as quickly as you can, even if you have to update the report later. This will help mitigate financial, legal, and reputational damage.

KEEP YOUR PLAN CURRENT

New technologies are regularly emerging to manage and analyse data, and businesses need to keep on top of these to incorporate them in their cybersecurity planning.

You can deploy new technologies, such **as AI and machine learning**, to improve your defences, but bear in mind, that actors will be doing the same to improve their attacks.

Cybersecurity will continue to be a game of cat and mouse, and it is vital that everyone maintains their vigilance at all times. In other words, businesses must strive to stay a step ahead of attackers.

CHOOSE YOUR DATA CENTRE WISELY

If you prefer to **outsource your systems** to a third-party data centre, remember that you are the customer and you have a right to ask searching questions about everything from their physical environment to their policies and procedures. Are you comfortable with who is allowed in your environment? Do you have an SLA that ensures you are notified about any breaches? Do you have audit rights? Are you confident that the provider is subscribing to frameworks such as ISO 27001?

CONSIDER YOUR SUPPLIERS AND PARTNERS

However good you are at cybersecurity, your business is not an island.

Look at your third-party connections, and try to treat them with the same sort of oversight and controls as you would for your own organisation – although this will not always be easy. Many companies are moving their critical systems away from the public cloud to colocation centres for this very reason.

6. IBM/Ponemon Institute: 2020 Cost of a Data Breach

FIND EXTERNAL HELP IF YOU CAN'T DO IT ALL YOURSELF

A third-party consultant can look at your assets, find out where they are, and determine how to classify them. They will conduct different threat models and determine the best ways to mitigate those threats.

Small and medium-sized businesses are unlikely to be able to maintain full-time security officers. **Find a partner instead**, who can come in a couple of times a year to review and advise. Keep them as a retained provider on speed dial, so that you have someone available to help in case of attack. Again, your cyberthreat insurer will probably be happy to point you in the direction of someone they trust.

The more you invest in a programme, the better it is likely to be. There are many firms who will not only go through training exercises, but will be able to test users to reinforce what they have learned.

If you are really not in a position to hire a third party, there are **online organisations**, such as SKA and IACPA, who can help. You can also find threat-assessment templates that you can use yourself.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 225,000 organisations around the world, and with a real estate network of nearly 93 million square feet across approximately 1,450 facilities in 56 countries, Iron Mountain stores and protects billions of valued assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure records storage, information management, digital transformation, secure destruction, as well as data centres, cloud services and art storage and logistics, Iron Mountain helps customers lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.

IRON MOUNTAIN®