Cybersecurity essentials for medium-sized enterprises

Barracuda

Executive summary

Medium-sized enterprises (MSE), which for this paper we are defining as businesses with £10m-£200m turnover and between 200 and 2000 employees, are attractive targets for cybercriminals, because they often form part of a larger company's supply chain and can be seen as a stepping stone to a more lucrative victim. Some MSEs will have grown faster than their security teams. Some may still have the security stance of a much smaller business. And some MSEs will be the result of rapid takeovers and mergers which may have left undocumented vulnerabilities in networks and shared systems.

The research that underpins Barracuda's Cybernomics 101 report found that almost half (48%) the companies with 100 to 750 employees describe their cybersecurity posture as fairly ineffective. This feeling is shared by 37% of those with 750 to 2,500 staff. Meanwhile, the median impact and recovery cost of IT asset damage ranged from around $50K to $100K for the smaller MSEs to up to around $1 million or more for the largest MSEs. These are significant costs for an MSE to shoulder.

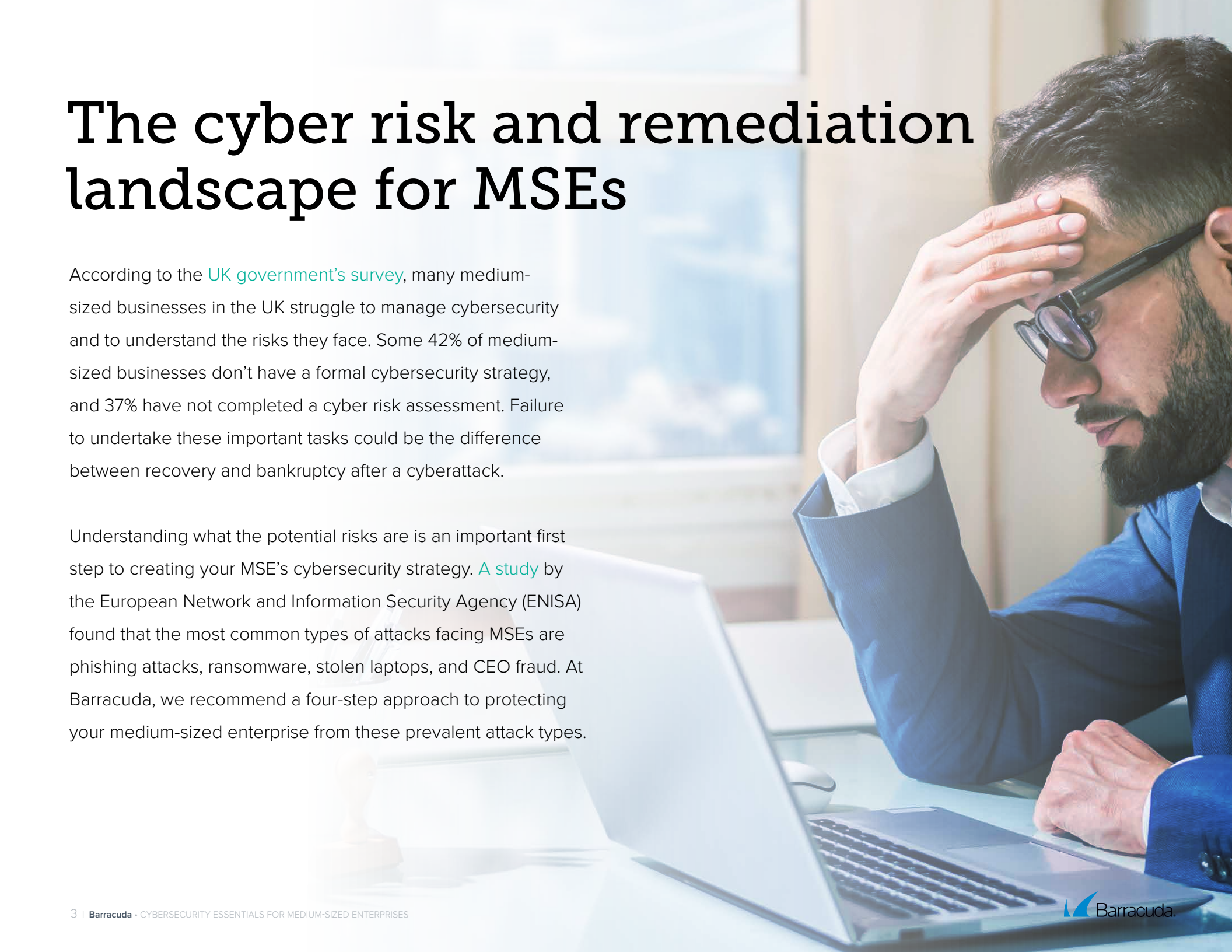
To limit and contain the impact and expense of an IT security incident, MSEs need to have a clear plan and measures in place to protect them from the potentially devastating consequences of an attack. We hope the following pages will inspire medium-sized enterprises to take action to protect themselves from today's cyber threats and protect their email, applications, network, and data.

Barracuda

The cyber risk and remediation landscape for MSEs

According to the UK government's survey, many medium-sized businesses in the UK struggle to manage cybersecurity and to understand the risks they face. Some 42% of medium-sized businesses don't have a formal cybersecurity strategy, and 37% have not completed a cyber risk assessment. Failure to undertake these important tasks could be the difference between recovery and bankruptcy after a cyberattack.

Understanding what the potential risks are is an important first step to creating your MSE's cybersecurity strategy. A study by the European Network and Information Security Agency (ENISA) found that the most common types of attacks facing MSEs are phishing attacks, ransomware, stolen laptops, and CEO fraud. At Barracuda, we recommend a four-step approach to protecting your medium-sized enterprise from these prevalent attack types.



Step 1: Protect your email

Email remains a highly attractive method of conducting cyberattacks, with phishing, spear-phishing, CEO fraud and quishing (QR code phishing) providing criminals with multiple methods to gain entry to a business via email. Medium-sized businesses are attractive targets for email attacks, as bad actors may assume that there are less rigorous cybersecurity practices in place than in large corporations. In this type of attack, attackers send fraudulent emails that contain a method of obtaining login credentials, or other sensitive information, which could allow them to gain access to your business' network and systems to extort money. Our eBook, 13 email threat types to know about right now, can help you learn the different ways bad actors can exploit email to compromise your business.

Barracuda's approach to email protection is a three-step process: prevent threats, detect and respond, and secure your data. Email threat prevention is an important factor and is multi-faceted. Perhaps the most important method of prevention is to educate your users. A phishing email cannot cause any damage to a company if nobody clicks on any links. The key here is to regularly and thoroughly train your staff to be able to identify phishing emails and to have a process in place for reporting any suspicious emails that find their way into your users' inboxes.

Tools that check email contents can assist in identifying malicious emails, but they shouldn't be seen as a replacement for training your staff to spot threats. These scanners use methods such as artificial intelligence (AI) to automatically scan every email in your inbox to detect malicious intent. They can also create reports that show you where you need to boost your security strategy based on the kind of threats that are making it through to inboxes. Email encryption is also an important part of the email protection puzzle. This protects sensitive information from anyone who doesn't have the decryption key, adding another layer of protection.

Step 2: Protect your applications

Another attractive entry point for malicious actors is your business applications. Medium-sized enterprises may have a range of different public-facing applications, including login and customer portals and e-commerce platforms for purchasing products. Applications like these are business-critical and contain sensitive customer and business data. If these are targeted, cybercriminals can cause significant damage to your business in many ways. Applications are vulnerable to distributed denial of service (DDoS) attacks, in which an attacker sends an excessive amount of bot traffic to overwhelm an application, taking it offline.

Forcing downtime and stealing data by injecting malware are two potential routes for cybercriminals to exploit your applications. According to Verizon's Data Breach Investigations Report 2024, the top motives for attacking applications are financial (97%) and espionage (3%). Applications themselves can be vulnerable to attack because they accept users connecting to them via insecure networks such as public WiFi, which is unencrypted. For these reasons, application security needs to be baked in from the beginning, not built on top as an afterthought.

Implementing a web application firewall (WAF) to monitor and filter traffic between the internet and web apps is one important part of protecting your applications. The WAF acts as a wall between sources of traffic and your application, filtering requests and blocking those that it identifies as malicious. Regular updates and patch management are vital for ensuring that the application is up to date and that any vulnerabilities have been detected and addressed. Unpatched weaknesses are an easy target for cybercriminals, so making sure you have a regular and thorough patch management schedule is important.

Monitoring your applications for suspicious activity is another key part of protecting them. This can help you identify any unusual traffic or behaviour that might indicate a potential attack, allowing you to respond accordingly. Having an incident response plan in place helps you face such an event with a strategy, rather than reacting haphazardly.

Step 3: Protect your network

Many medium-sized businesses employ people who work in various locations, and not in offices. With the rise of remote working and even “work from anywhere” policies, the network perimeter has expanded in ways that make it more difficult to protect. Staff are connected to business systems and one another via cloud applications and communication software, which are themselves potential entry points for bad actors. And with bring-your-own-device (BYOD) policies, until you implement a rigorous and repeatable device security strategy, there will be varying levels of protection — if any at all. Making sure that all devices are secured to the same rigorous standard is vital.

Medium-sized enterprises need to employ best practices to secure the perimeter and create a fortified barrier around their networks to protect and connect people, sites, and things. Secure Access Service Edge (SASE) is one such approach to network security that consolidates security functions and centralises cybersecurity management, improving a company’s overall business posture. It combines network protection functions with Wide Area Network (WAN) capabilities to support the secure access needs of today’s businesses.

Zero Trust Network Access (ZTNA) is another approach that helps to protect your network by using the philosophy “never trust, always verify.” It grants access to different assets and parts of the network on a case-by-case basis, giving access only to those who need it and verifying in each instance that it is these users who are attempting to gain access. ZTNA offers a way to securely connect users to your network no matter where they are located, which is perfect for companies with distributed workforces.

Step 4: Protect your data

Data is a coveted asset, and cybercriminals go to many lengths to seize it. Businesses with weak data protection face the risks of fraud and extortion. With phishing and ransomware attackers attempting to steal data to exploit businesses of all sizes, mediumsized enterprises need to apply strict data protection policies, even if they don't think all of their data is sensitive.

Regular backups are essential, protecting your data in the event of damage or loss of hardware and adding a protective layer against attacks such as ransomware. With regular, complete backups, you can restore your data at will, regardless of the ransomware attacker's actions. ZTNA helps to protect your data too, by ensuring that data is only accessible to people with the necessary permissions.

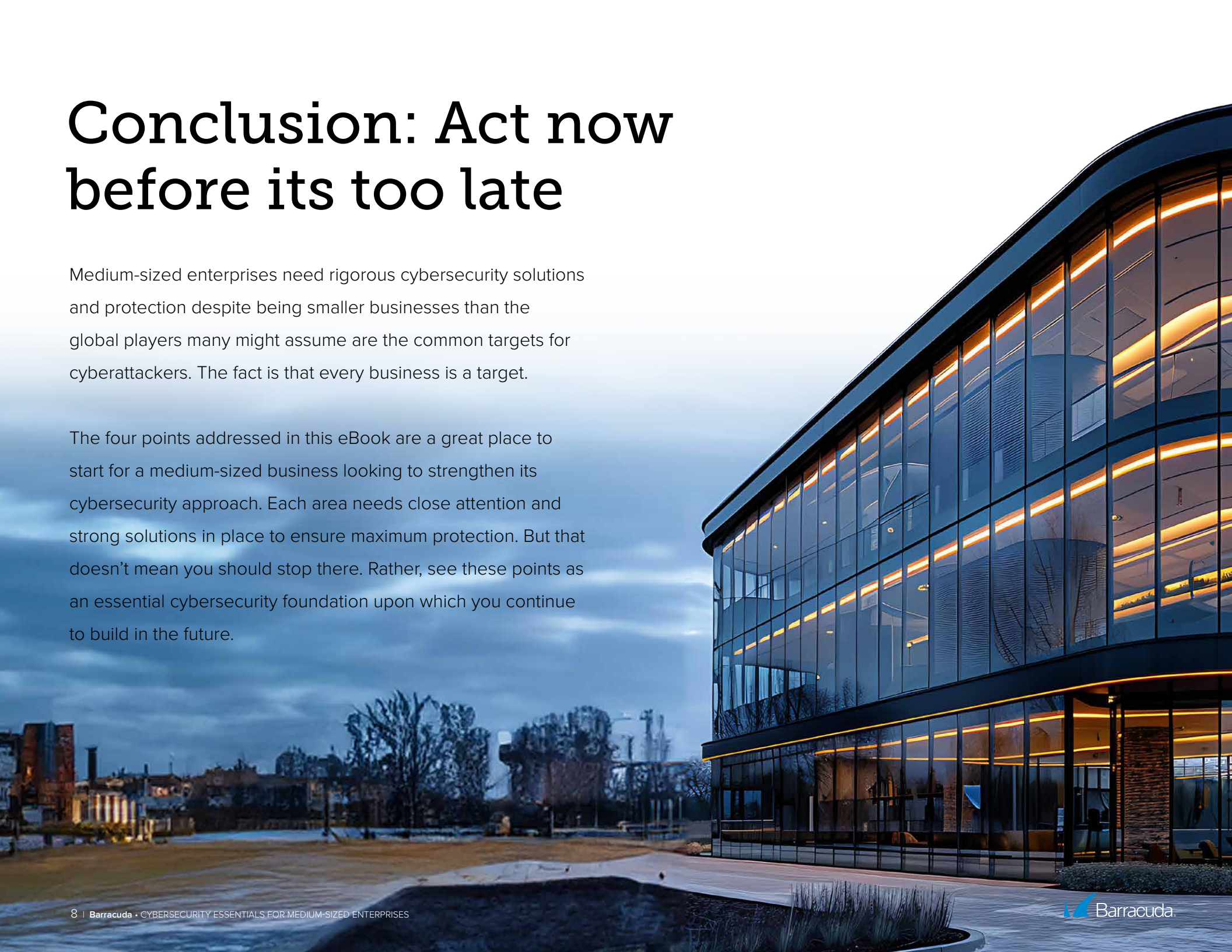
Organisation-wide mindsets, education, and training are also vital aspects of protecting your business data. Even medium-sized enterprises must operate with the mentality of when, not if, they will be hit by a cyberattack, and should train staff appropriately. This includes education about password policies, as weak passwords are a common way for attackers to gain access to data.

Barracuda

Conclusion: Act now before its too late

Medium-sized enterprises need rigorous cybersecurity solutions and protection despite being smaller businesses than the global players many might assume are the common targets for cyberattackers. The fact is that every business is a target.

The four points addressed in this eBook are a great place to start for a medium-sized business looking to strengthen its cybersecurity approach. Each area needs close attention and strong solutions in place to ensure maximum protection. But that doesn't mean you should stop there. Rather, see these points as an essential cybersecurity foundation upon which you continue to build in the future.



About Barracuda

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organisations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level. For more information, visit barracuda.com.