SecureAge

Cybersecurity for SMEs – applying a Data-centric lens

SecureAge Whitepaper 2021

Summary

In this report we will review:

- **How low data security awareness among SMEs constitutes a market failure: 66% of small business owners do not believe they will fall victim to a cyberattack and yet the number of small businesses facing data breaches increased 63% in 2019 alone.**
- **How ineffective and risky 'band-aid' data security solutions are being thrown at small businesses – staff training, cloud technology and cyber insurance – and why this is putting more and more SMEs in danger.**
- **How we have helped SMEs around the world with simple advice and an approach that focuses on data to achieve 100% protection without excessive financial investment, reliance on humans, or need to overhaul existing infrastructure or ways of working.**

Data loss happens, a lot! Hardly a week passes without news of a data security breach at a well-known multinational corporation. Either company or consumer data is being taken by a disgruntled employee, malicious insider, or professional hacker. In fact, it's become so common that we're almost at the point where these events are quickly forgotten by the press and public. That is until the next big corporate hacking episode takes centre stage. Amidst that cycle, however, it is concerningly uncommon to hear anything about the very many small businesses that are suffering the same data breaches and malware attacks.

There is a simple reason - cyberattacks are deadly for SMEs

If a small business suffers a data breach or cyberattack, it rarely stands a fighting chance of surviving long enough to ever become newsworthy. For an SME, a data breach, or loss, is life or death.

This differs from bigger firms that can approach ransom demands and fines as a simple business decision. Large enterprises simply have the luxury to choose to invest in data security solutions before a cyberattack happens or spend the money after an attack happens on ransoms, penalties, and fines. Unfortunately, the least able to cope are the most likely to suffer cybercriminal activity.

The bigger problem, however, is that these small businesses which are most in need of accurate information about data security are the least well informed. A lack of awareness of the likelihood, as well as the impact of a data breach exists among small business owners. This creates a distorted reality.

The numbers don't lie - data breaches among SMEs exist

> - A study by the Ponemon Institute shows that the number of small businesses facing data breaches increased by 63% in 2019.
> - In another report by Verizon, one in three data breaches involved small businesses.

And yet, in the 2019 SMB Cyberthreat Study, which surveyed over 500 senior decision makers at small businesses, it was found that 66% of small business owners believe they will not fall victim to a cyberattack.

This mismatch proves that many promising SMEs are highly likely to be operating without meaningful security solutions and are at risk. This is concerning not only for the owners' livelihoods and the businesses growth potential, but also for the economies in which they operate.

Why are small businesses unaware of the security risks they face?

Globally, small businesses represent the largest group of employers and economic contributors. According to the World Trade Organisation, SMEs represent over 90% of the business population, 60-70% of employment, and 55% of GDP in developed economies.

Despite their importance to the global economy, small businesses have a misguided view that data breaches and cyberattacks only happen to big multinational corporations.

Truth be told, the myth is perpetuated by major cybersecurity firms as they are financially motivated to chase data security contracts with large enterprise customers or governments. By focusing their investigations and reports on large enterprises, they are able to generate media coverage that enables them to secure these bigger contracts.

It's no different from the paparazzi trying to get front-and-centre for the latest celebrity breakup story. However, the widespread circulation of this gossip does not mean that a much greater number of breakups don't happen among us regular folk – they just don't get as much coverage.

Why would a hacker target a small business?

You might still be wondering what would motivate hackers to target a small business. After all, bigger brands have more customers, so it seems to make sense that hackers have more to gain from targeting these larger entities.

The reality is quite different. Most small businesses are targets of opportunity; they are not necessarily carefully planned. As such, an attack on a small business tends to be more generic in nature and run autonomously. But don't be mistaken - this doesn't mean they are any less damaging than a well-organised and usually well-funded targeted attack.

Hackers are aware that most small businesses do not have the resources or security solutions in place to detect time-bombed ransomware. This means that a cybercriminal could easily be inside an organisation's network, preparing for data destruction or planting ransomware without them knowing. The ensuing ransom demand would be issued days or weeks later, well before the business owner becomes aware of the situation.

The report by the IBM-Ponemon Institute in 2019 shows it takes an average of nine months for small businesses to discover and remediate a data breach. And even if the cyberattack is detected, these businesses typically do not have the resources or security software in place to halt the attack, let alone to remediate it.

Big firms, on the other hand, usually have in-house capabilities on standby 24/7, or contracts with third-party security operation centres. This, combined with the fact that these teams have generally learnt the ways of cybercriminals, acts as a deterrent.

Sure, data breaches are still common among large businesses but SMEs have become easier targets. Hackers know that without effective and proactive data security solutions, these businesses can't defend themselves.

Internal security threats are also dangerous for SMEs

It's not just external professional cybercriminals that small businesses have to worry about. Small businesses often face disgruntled staff, clients, and industry rivals who also have the potential to cause harm. This makes sense as naturally insiders have easy access to company files.

Over our 18 years in the cybersecurity industry, we've found that the majority of data that is stolen from SMEs is taken by someone inside the organisation. In fact, most of these data breaches occurred because information was simply left exposed and therefore unprotected on the internet.

But it even goes one-step further than employees. Today, it's also common for customers, suppliers, and business partners to have access to the organisation's data in some form. Of course, we're only human and humans make mistakes.

If you add to this the fact that it's as affordable and easy as ever for disgruntled stakeholders to buy keystroke loggers, IoT and webcam exploits, as well as the rise of ransomware-as-a-service, we simply have to conclude an unfortunate truth: existing security solutions are failing SMEs.

'Can't we just try harder or rely on external experts?'

This is indeed the type of advice that is often thrown at most small business owners. Unfortunately, this 'band aid' approach only places more and more small business owners in the red while leaving them vulnerable to cyberattacks.

When it comes to SMEs, the usual cost of implementing a pro-active security solution is something that most business owners want to defer. The lure of lead generation services, award applications, and software to increase productivity appears to offer more immediate returns. Of course, your return on investment is an important metric, but there will be no return to measure if the company can't survive a cyberattack.

Cybersecurity for small businesses – what not to do

Before covering our approach, allow us to first dispel some common cybersecurity myths:

1. You can't build a truly effective cybersecurity culture

Many small business owners are led to believe expert advice. And many experts advocate the creation of a cybersecurity culture and become laser focused on training teams on cybersecurity best practices. But how exactly is this done?

The usual recipe is to identify known vulnerabilities and exploits, download patches and updates, or buy promises from cybersecurity product and service vendors. The next step involves listing up the relevant security skills and disciplines that employees need to learn and adopt, and then train, test, and repeat.

It sounds easy enough, but with every new hack of some notoriety, those skills need updating and that means even more training and more testing. It becomes an endless game of cat and mouse that most often results in confused, jaded, or even nervous employees - especially when a mistake or failing internal spot-testing could result in job loss.

Building a cybersecurity culture takes a lot of work. Without even considering the need for constant vigilance and attention to all potential threats worldwide, we need to remember the people we employ are human, and humans will always make mistakes.

Building an ambitious cybersecurity culture also requires employee buy-in and more often than not, our employees were hired for a different task and they do not see data security as their job. Besides, everyone knows that anything that requires long explanations, training sessions, or even worse – a manual, tends to get in the way of business.

We're not suggesting it's not important to arm your teams with cybersecurity tools and knowhow. But we are suggesting that a small business should not rely on administrative and physical controls that require your team members to become cybersecurity experts or which get in the way of the task they were hired for.

Even if you are able to hire security professionals, is there any amount of training that would allow anyone to defend themselves against a motivated hacker with a limitless realm of technical and social engineering tricks up their sleeve?

2. The cloud isn't going to fix all of your cybersecurity issues

As we write this, almost every industry is in a state of flux. Getting through a tumultuous 2020, it's accepted that the world will never go back to how it was before 'COVID-19' became part of our everyday vocabulary. This 'new normal', as the media has termed it, has mandated a meteoric rise in the reliance on cloud environments.

For some industries, it is indeed an exciting time – crises can breed innovation. But innovation can also expose security gaps, and that's what's happening with the cloud. It's not that cloud technology itself is at fault – although it can introduce liabilities to your data – it's that you're relying not only on your own staff but also on those at your cloud provider to bolt all the doors properly.

You may have seen in the news that in 2017 a security researcher discovered four unprotected Amazon S3 storage buckets containing highly sensitive data, including client credentials at Accenture. This occurred because the buckets had been accidentally set to allow public access.

Accenture isn't alone. Since then, many other companies have reported cloud-based data security lapses where data was left exposed to the public. This includes Dow Jones, Verizon, and the military intelligence agency INSCOM.

The problem with both cloud-based and locally stored data security is that it is typically protected using security 'door'. If the security door – in the guise of authentication and access controls – is left open, bypassed, or breached, then the stored data is there for the taking.

3. Cyber insurance checks the boxes but may not save your business

Sadly, many businesses have also been led to believe that it will be cheaper to buy insurance than to invest in pro-active data security solutions. While cyber insurance does seem tempting, the cold truth is that no premium can provide a small business with the coverage it needs.

Those relying on cyber insurance are misguided and unaware of the fine line that exists between what is preventable and what we have no control over. Many small business owners are unaware that proof of the best security practices having been followed will need to be shown to investigators before any claim is paid. Naturally, proving that you have done so is a long, tedious, and expensive process that most small businesses are unable to endure. Not only do you need in-depth knowledge of cybersecurity solutions, but you also need legal expertise.

Other questions to ask are, even though the insurer may pay the fines and cover the PR bill, will that keep a small business afloat when systems are down or reputations damaged forever? How important is the company's reputation when it comes to sustaining sales? How important is your business to your insurer? When we ask these questions, it becomes clear that preventing the data breach in the first place is the better route.

Tried and tested cybersecurity solutions can't be trusted

As small businesses race to launch new initiatives, speak to new audiences, and differentiate themselves through digital innovation, one common threat remains: data security. One simple lens can make the difference. Whether you're an SME in Africa, or a multinational in London, securing the lifeblood of business – data – is an efficient and effective cybersecurity solution.

Unfortunately, the industry has painted the illusion that data security is a tough business. Sure, it has a lot of moving parts, but we think Visa's founder Dee Hock said it best.

> 'Simple, clear purpose, and principles give rise to complex and intelligent behaviour. Complex rules and regulations give rise to simple and stupid behaviour'.

We couldn't agree more. That's why we're rattling the security industry with a simple solution for SMEs that places data security and usability on an equal footing.

We've achieved this by holding strong reign on our principles that data encryption should be inherent, invisible, and instinctive. With our SecureData encryption technology and the SecureAge Security Suite, our data security software, we ensure that all data is protected all the time. That includes when data is in-transit, in-use, and at-rest (ALL three states).

The rule book has needed to be revisited and updated for some time. That's the very reason why we championed a new data security solution that adds value for small businesses without excessive financial investment, reliance on humans, or need to overhaul existing infrastructure or ways of working. It just so happened that our prediction was correct and now more than ever, this is the type of security solution that small businesses need.

SecureData encryption technology in action

As a design and testing hub, one of our North American partners needed assurance that any new solution could protect 100% of their data. A data breach of any kind would put their engineering efforts and valuable IP at significant risk. In the wrong hands, even the exposure of a scheduled lunch meeting could provide a pathway toward getting access to other confidential data.

Proud of their hard-earned reputation and growth, and yet aware of the risk of sabotage and cyber espionage in their highly competitive industry, our partner began a search for a proven data security solution suitable to their environment with the following requirements:

- **A security solution that would protect their data from both internal and external threats.**
- **A solution that could accommodate their relatively small size (+40 workstations and servers), but still scale as they grow.**
- **A solution that is affordable and easy to implement without the need for a dedicated IT department or more infrastructure.**

After comparing various approaches, they recognized that powered by SecureData encryption technology, the SecureAge Security Suite was the perfect solution. SecureData protects every file, every place, every time without interfering with existing systems or employee processes and without the need for additional infrastructure. It's also supported by an 18-year history of ZERO data breaches in the toughest environments in the world.

The bottom line: small businesses deserve better cybersecurity tools

The demand for proactive cybersecurity and data security solutions for small business has risen, and it's not because regulatory measures require it. To a certain degree, it's not even because the threats have increased – threats will always be there. It's because existing solutions are simply not working.

The scary part about this is that the spotlight continues to be shone on multinational firms, while the increasing number of data security threats that small businesses face is ignored. Here's the stories we don't see:

- **The story of the local lawyer unable to use their computer system for a week due to a destructive malware attack.**
- **The story of the insurance broker whose confidential client details are being held ransom.**
- **The story of the advertising agency owner who wakes up to find their bank account wiped clean.**

The fact that these attacks do not appear on our newsfeeds does not mean they're not happening.

It's been said that 'consumer-friendly' was the calling card of the post 2008 crisis so perhaps in the aftermath of 2020 pandemic crisis, 'data-friendly' will finally be treated with the urgency that it needs. It's why the heads of the major U.S. banks stressed the importance of cybersecurity to Congress last year, and it's why the European Union issued the first ever sanctions against cyberattacks in July 2020.

Data security should never have become so complicated. With the SecureAge Security Suite, small businesses, governments, and multinationals alike can finally - proactively and effectively - protect their data by skipping the complexity.

Stay safe, stay secure.

To find out more about our SecureData encryption technology visit here.

To find out more about our data security software, the SecureAge Security Suite visit here.

To share your thoughts, see a demo, or discuss partnership opportunities, reach out to us directly at protect@secureage.com.

Website www.secureage.com
Contact protect@secureage.com

SecureAge

Singapore 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
United Kingdom 74 Mackie Avenue, Brighton, BNI 8RB, Company No. 11734665
Japan 1-16-6, Toranomon, Minato-ku, Tokyo 105-0001, Japan
North America 1801 Old Reston Ave Suite 301 Reston, VA 20190, USA