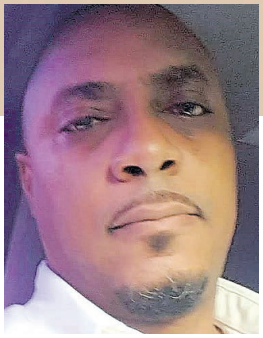
Five ways to protect business data

Encrypted data is one of the ways businesses can protect their information. (Internet image)



Roger Nicholls (GP)

By Roger Nicholls

The impact of COVID-19 on businesses in Barbados has reset the rails for the information technology (IT) services industry that supports them.

With much of, if not the entire, world in lockdown to reduce the spread of COVID-19, business levels are falling and island economies are heading for recession, ours in Barbados being no different than anywhere else in the world.

There still remains an idea within some small and medium-sized businesses (SMBs), especially here in Barbados, that they are too small to be attacked because there is less value in their information. It is simply not true. In fact, small businesses are more likely to be targeted with a ransomware attack. According to Infrascale, 46 per cent of all small businesses have been the targets of a ransomware attack.

For SMBs, security is crucially important for its success. It is very easy for any SMB to fail if it does not care about its security. Following some of these tips mentioned is a good start and can protect your business from basic attacks.

1. Have a security policy

When it comes to IT security, make sure your business has a policy, have it documented and available for all employees. Most of all, start with just the basics. Use complex passwords, don't open emails from suspicious addresses and don't open links from sources you don't recognise.

2. Train your employees

All employees should be trained to never hand out sensitive information to anyone they don't recognise. Make security awareness training part of your onboarding process and repeat this annually. The majority of small businesses suffer from phishing or spear-phishing attacks. These often come in the form of emails and these hackers can make themselves appear very real to recipients.

3. Encrypt your sensitive data and communication

Encryption simply means changing your data into an unreadable state. Using a simple program such as WinRAR is a good start. Take it a step further by having encrypted data and password protected on different office computers.

A small business most likely won't have an in-house encryption expert, but there are plenty of technology solutions that will encrypt data for you.

4. Install patches and updates

Operating on an outdated version of software can be dangerous. Please don't ignore software updates when they're rolled out, as they can contain security patches to vulnerabilities that hackers exploit.

The older the system is, the more serious this issue is. For example, it probably won't be too much of an issue if you miss the latest update for Windows 10, but if you're still running on Windows 2000, we'd recommend you upgrade immediately.

5. Consider using two-factor authentication

Sometimes referred to as a two-step verification or dual-factor authentication, this is a security process in which users provide two different authentication factors to verify themselves. This process is done to better protect both the user's credentials and any resources that user can access.

While most Caribbean small businesses won't find themselves victims of data breaches, every single SMB should still be concerned about their information security. This is especially important if your business handles consumer data.

Please be mindful of the breach experienced when ANSA McAL fell victim to a ransomware attack when hackers held some of ANSA's IT systems hostage while reportedly demanding payment. This attack was perpetrated on one of the largest conglomerates in the Caribbean region.

The unfortunate truth is that cybercriminals are exploiting the situation of the COVID-19 pandemic to launch highly sophisticated cyberattacks on every industry possible. It really is not about the size of the company as some business owners want to think. It's about the data and how that data can be exploited and sold on the Dark Web.

In the first six months of 2020 alone, companies became the target of massive data breaches where hackers sold account credentials, sensitive data, confidential and financial information of these organisations.

We understand that data security is hard and "securing data" is thought to be as easy as storing it on a portable hard drive and "that's all you need right now". The budget pressures of SMBs are unique. We've sat and had those difficult conversations with business owners and we've also had to ask those difficult questions: "Are they fully protected?" "What is most critical to their business?" "What would downtime really cost per hour for their business?"

Cybersecurity report

Almost a third or 28 per cent of the data breaches in 2020 (until now) involved small businesses. The data comes from one of the most acclaimed cybersecurity reports in the industry, the **Verizon Business 2020 Data Breach Investigations Report (2020 DBIR)**.

Now, with many companies still being impacted by COVID-19 restrictions, SMBs can easily find themselves being ill-prepared to fully address those security issues.

Though all is not lost for SMBs, the data protection principles and the technical tools are there to allow them to strike the right balance going forward in a post-COVID-19 environment.

SMBs should not have to risk higher threats of breaches just because of their size. The answer lies in not waiting until disaster strikes, but in being proactive.

Roger Nicholls is the lead information technology consultant of Digital Networking Solutions, and has more than 12 years of IT enterprise experience.

Good cyber security has layers

by Roger Nicholls

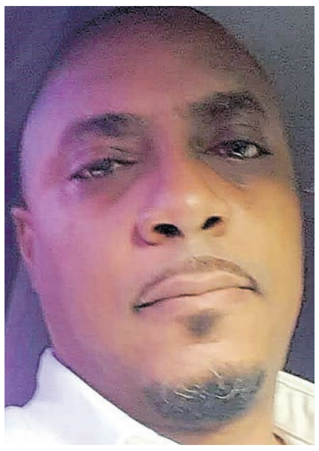
The best cyber security solutions have many layers. (Internet image)

A successful small and mediu- sized business (SMB) focuses on two things above all: growth, and a shrewd oversight of cash flow. This makes them attractive targets for cyber criminals, and in this modern age, weak security can put a stop to both of these things.

Layered security is generally the best defense in the face of current and future threats to your small business. Within this framework, you will hear two solutions discussed frequently as solutions to protect your business or your end users: managed antivirus (MAV) and endpoint detection and response (EDR).

But no small business owner really cares about MAV over EDR or vice versa. The questions usually asked most often are: How will this software impact on my return on investment?, and, What's the long-term cost on my business if we implement this?

My technical disclaimer is that neither is a one-size-fits-all solution. They both address different issues. When discussing on deciding between the two, it's important to consider several factors, including the type of business in need of protection, which end users really need either solution, and lastly the cost attached to either solution.



Roger Nicholls (FP)

Why your business needs managed antivirus

It is solid protection at a great price point, and a centrally-managed software option that can protect all of the computers in your business from virus threats. With MAV, information technology solutions providers are able to handle your virus definition updates – so user intervention really isn't necessary. When a virus or malware is discovered, it's immediately quarantined.

It's a simple, straightforward first line of defense for your small business – it doesn't require any technical knowledge and does a good job of turning away many threats. However, MAV requires regular definition (virus signature) updates and therein lies the "chink in its armor".

With new threats arising almost daily, ensuring updates getting "pushed out" in a timely fashion is truly a best-effort scenario. The protection afforded by the MAV is only as good as the anti-virus vendor's latest updates; threats in some unfortunate cases are sometimes only discovered after the damage is already done.

So why choose MAV for your business? Clearly, ease of use is at the top of the list. It's a good value proposition at an affordable price point. Some additional benefits include:

● One centralised management source: The SMB owner can look to their solutions provider as the single source for deployment, management, definition updates, and threat debriefings.

● 24/7 monitoring: You set the scan schedule, update the software, and push out definition updates. It doesn't require any intervention from yourself or your end users.

● Fast remediation: Your solutions provider is able to triage and respond to your threats in real-time.

● Cost: MAV is less expensive than EDR. This is the second biggest selling point for MAV beyond the effective protection aspect. But the margins are becoming slimmer. And given the threat environment we face today; your business might be in a position where it can't afford not to pay for EDR.

Endpoint detection and response

EDR is a multifaceted solution that does everything modern MAV can do, but takes things a step further – in providing greater security. EDR is centred on endpoint protection. As with MAV, a solutions provider can manage it without requiring any input from the end user (SMBs). Given the number of threats that do spawn almost daily, managing large numbers of endpoints can be more difficult with antivirus and other point solutions. At this point the differences between MAV and EDR come into sharp focus.

When we talk about traditional MAV, it's typically from a passive standpoint. MAV can only detect and quarantine known threats – those that have been previously identified. MAV requires regular signature updates. This means there is often a gap in coverage between when a virus is discovered and when your small business can become protected. Plus, threats that haven't yet been discovered can operate in the wild before you can even get an update. It's a reactive approach with proactive intent.

This is in total contrast to EDR, which is proactive. Comprised of monitoring software and endpoint agents, EDR solutions use integrated machine learning and advanced artificial intelligence (AI) to identify suspicious behaviours and address them regardless of whether or not there's a signature. For example, if several files change at the same time, chances are it's more likely a result of an endpoint assault rather than user error.

COVID-19 has changed the business environment, from the rise of e-commerce to business solutions that millions of individuals will rely on daily. But with this progress comes inevitable roadblocks, and for the small business owner, they must focus on intent – those who look to profit from them in harmful ways. Data is arguably going to become your small business' greatest asset.

You have options and you should always consider your own business needs. EDR is perfect for managing sensitive human resource data – such as your company payroll. But it may not be necessary for someone who simply stores personal files in the cloud or has MAV. One size in this case does not fit all.

A solid layered approach to your business security is always recommended so make sure to patch and back up regularly.

Roger Nicholls is the lead information technology consultant of Digital Networking Solutions, and has more than 12 years of IT enterprise experience.

Managed IT services help businesses

There are various reasons why businesses should consider managed information technology systems. (internet Image)

By Roger Nicholls

As small and medium sized businesses (SMBs) in Barbados reopen and recover, the ability to operate differently is becoming clear and critical in our new normal where the current pressure on traditional business models has been exacerbated by the COVID-19 pandemic. While none of us would have foreseen COVID-19 in our business forecast, the truth is that our traditional SMB business models were already feeling the pressures of a shifting technological business world.

The sad fact for us in Barbados is the COVID-19 pandemic has laid bare the inadequacies of current technology solutions in our SMB community driven by years of postponing investment in technology and utilising manual workarounds. This is not at all a scathing attack on business owners as we empathise with SMB owners who have to balance the difficult task of securing their business objectives against balancing the costing of securing their data or their systems.

However, consider some of the following questions. Do we have the ability to keep our devices up to date and patched to avoid any potential security risks? Have we done the necessary due diligence to test our network for potential internal and external vulnerabilities? If we were to have a breach, do we have the capability to find and remediate it on our own? If a lightning strike caused a national shutdown, frying our hardware tomorrow, do we have a plan to get back up and running? And even if we have a plan, have we actually tested it to make sure that it's viable?

An information technology (IT) managed services provider can offer assistance and expertise to SMBs.

Roger Nicholls (FP)

As a third-party contractor, an IT managed services provider can assume all or some of the role of an IT department, such as monitoring their client's network, optimising their client's infrastructure, or protecting the overall system from any security threats. If the SMB does have in-house IT staff or an IT person, those services may be used to supplement their capacity and allow them to focus on particular functions, or to provide specialist knowledge in areas where they are lacking – such as managed backup or cloud services.

Some of the tasks and monitoring services that businesses can explore include:

Network and system monitoring

Monitoring your own network can be a time-consuming task for any SMB. An IT managed services provider can take on the role of monitoring your organisation's network performance, quality, and downtimes, remediating their issues quickly when they arise – often before end users realise there is even an issue. Over time, the data gathered helps the business owner improve their infrastructure, optimise their performance, and reduce costs and allows a streamline to better productivity.

System design and upgrades

This involves working with individual businesses to understand their unique requirements and ensuring that their IT systems fully support their business objectives. As part of this, you'll need to keep an eye on more general industry trends to make sure clients remain on the cutting edge. As an IT managed services provider, you may be required to set up cloud or other outsourced infrastructure, wireless and mobile networking, and virtualisation solutions.

Security management

This is protecting your business against the latest malware threats, providing software patching and maintenance, monitoring application compatibility, and performing other parts of risk protection and cybersecurity. It also includes managing your business email security and helping to safeguard your most sensitive data from ransomware attacks.

Backup and disaster recovery

Ensuring the integrity and safety of a company's data is another key role managed services providers fulfill. Making sure that they have adequate backups and that data is able to be recovered in the event of a disaster is critical to this.

Communications, support, and software as a service

Some IT managed services companies can choose to offer communications support such as data, Voice Over Internet Protocol, or video as part of the provided and managed services package. Others will be able to support software applications that are hosted on their own servers and offered on a subscription basis.

Auditing and compliance

A managed services provider removes the compliance burden for their clients with thorough assessments. When it comes to network vulnerabilities, logging practices, cloud computing, and industry-specific policies, it's important to provide appropriate guidance and support around compliance.

In the post COVID-19 era, every modern business environment can have a security risk and could potentially be vulnerable to some form of attack. As such, it's crucial SMBs make use of a security solution that is able to monitor every single device for threats such are ransomware and spoofing attacks. The solution your small business chooses should also be able to alert your IT team to any suspicious activity or potential problems.

Manually enforcing security standards and policies across even a small number of devices can be a challenge for any SMB – which is why it's important for SMBs to leverage IT solutions that can help them manage and monitor their systems in a unified and coherent way.

With cybercriminals becoming more sophisticated in their attempts to access SMB systems and data – and with companies taking on more IT assets than ever as organisations increasingly shift to remote work during the COVID-19 pandemic, managed services can be a valuable resource for SMBs, providing their expertise and experience.

Managed services aren't about convincing the client to buy the latest shiny technology product. The right managed services provider has to also be willing to be a long-term strategic partner that you the client can trust to have your best interests in the growth of their business at heart.

Roger Nicholls is the lead information technology consultant of Digital Networking Solutions, and has more than 12 years of IT enterprise experience.

Good cyber security has layers

by Roger Nicholls

The best cyber security solutions have many layers. (Internet image)

A successful small and mediu- sized business (SMB) focuses on two things above all: growth, and a shrewd oversight of cash flow. This makes them attractive targets for cyber criminals, and in this modern age, weak security can put a stop to both of these things.

Layered security is generally the best defense in the face of current and future threats to your small business. Within this framework, you will hear two solutions discussed frequently as solutions to protect your business or your end users: managed antivirus (MAV) and endpoint detection and response (EDR).

But no small business owner really cares about MAV over EDR or vice versa. The questions usually asked most often are: How will this software impact on my return on investment?, and, What's the long-term cost on my business if we implement this?

My technical disclaimer is that neither is a one-size-fits-all solution. They both address different issues. When discussing on deciding between the two, it's important to consider several factors, including the type of business in need of protection, which end users really need either solution, and lastly the cost attached to either solution.

Roger Nicholls (FP)

Why your business needs managed antivirus

It is solid protection at a great price point, and a centrally-managed software option that can protect all of the computers in your business from virus threats. With MAV, information technology solutions providers are able to handle your virus definition updates – so user intervention really isn't necessary. When a virus or malware is discovered, it's immediately quarantined.

It's a simple, straightforward first line of defense for your small business – it doesn't require any technical knowledge and does a good job of turning away many threats. However, MAV requires regular definition (virus signature) updates and therein lies the "chink in its armor".

With new threats arising almost daily, ensuring updates getting "pushed out" in a timely fashion is truly a best-effort scenario. The protection afforded by the MAV is only as good as the anti-virus vendor's latest updates; threats in some unfortunate cases are sometimes only discovered after the damage is already done.

So why choose MAV for your business? Clearly, ease of use is at the top of the list. It's a good value proposition at an affordable price point. Some additional benefits include:

● One centralised management source: The SMB owner can look to their solutions provider as the single source for deployment, management, definition updates, and threat debriefings.

● 24/7 monitoring: You set the scan schedule, update the software, and push out definition updates. It doesn't require any intervention from yourself or your end users.

● Fast remediation: Your solutions provider is able to triage and respond to your threats in real-time.

● Cost: MAV is less expensive than EDR. This is the second biggest selling point for MAV beyond the effective protection aspect. But the margins are becoming slimmer. And given the threat environment we face today; your business might be in a position where it can't afford not to pay for EDR.

Endpoint detection and response

EDR is a multifaceted solution that does everything modern MAV can do, but takes things a step further – in providing greater security. EDR is centred on endpoint protection. As with MAV, a solutions provider can manage it without requiring any input from the end user (SMBs). Given the number of threats that do spawn almost daily, managing large numbers of endpoints can be more difficult with antivirus and other point solutions. At this point the differences between MAV and EDR come into sharp focus.

When we talk about traditional MAV, it's typically from a passive standpoint. MAV can only detect and quarantine known threats – those that have been previously identified. MAV requires regular signature updates. This means there is often a gap in coverage between when a virus is discovered and when your small business can become protected. Plus, threats that haven't yet been discovered can operate in the wild before you can even get an update. It's a reactive approach with proactive intent.

This is in total contrast to EDR, which is proactive. Comprised of monitoring software and endpoint agents, EDR solutions use integrated machine learning and advanced artificial intelligence (AI) to identify suspicious behaviours and address them regardless of whether or not there's a signature. For example, if several files change at the same time, chances are it's more likely a result of an endpoint assault rather than user error.

COVID-19 has changed the business environment, from the rise of e-commerce to business solutions that millions of individuals will rely on daily. But with this progress comes inevitable roadblocks, and for the small business owner, they must focus on intent – those who look to profit from them in harmful ways. Data is arguably going to become your small business' greatest asset.

You have options and you should always consider your own business needs. EDR is perfect for managing sensitive human resource data – such as your company payroll. But it may not be necessary for someone who simply stores personal files in the cloud or has MAV. One size in this case does not fit all.

A solid layered approach to your business security is always recommended so make sure to patch and back up regularly.

Roger Nicholls is the lead information technology consultant of Digital Networking Solutions, and has more than 12 years of IT enterprise experience.