Small Medium Business Cyber Security Top Tips Using The PROTECT Protocol™

Let us start by asking some simple question. Does your business process data?

How long your business would operate if you did not have access to your data?

No matter if it is a list of customer information, supplier information, transactional information or other, all businesses rely on data. You need to accept that the number 1 asset in the world right now is not gold, silver or oil. It is data/information. Lose your data, risk losing your business. Therefore, it does not matter whatever size you are, nor what industry you are, as a small medium business (SMB) data security should be on the top things to discuss with your senior management or board every month. If not, this is a problem, and your first top tip is to get data security visible and discussions going with top management.

There are many areas you can do to improve security. You can become bombarded with information, or you could spend hours looking on YouTube or on Google, and it is no surprise that many businesses still do not make the right progress on their security journey.

During my time over 25 years in security and doing many data security and data compliance assessments for many organisations, and with challenges for remote working, I got busy. And I discovered something very exciting – I found a pattern emerging where businesses just got stuck, and what we could do to help them get securer, faster, and better. In fact, there exists right now a way to improve your security and protect your business against the worst from happening.

- ✓ Without having to in-depth technical knowledge of systems.
- ✓ Without being a large organisation with large budgets for investment.
- ✓ Without worrying are the right things protected enough.
- ✓ Without worrying what to do next in a security incident.

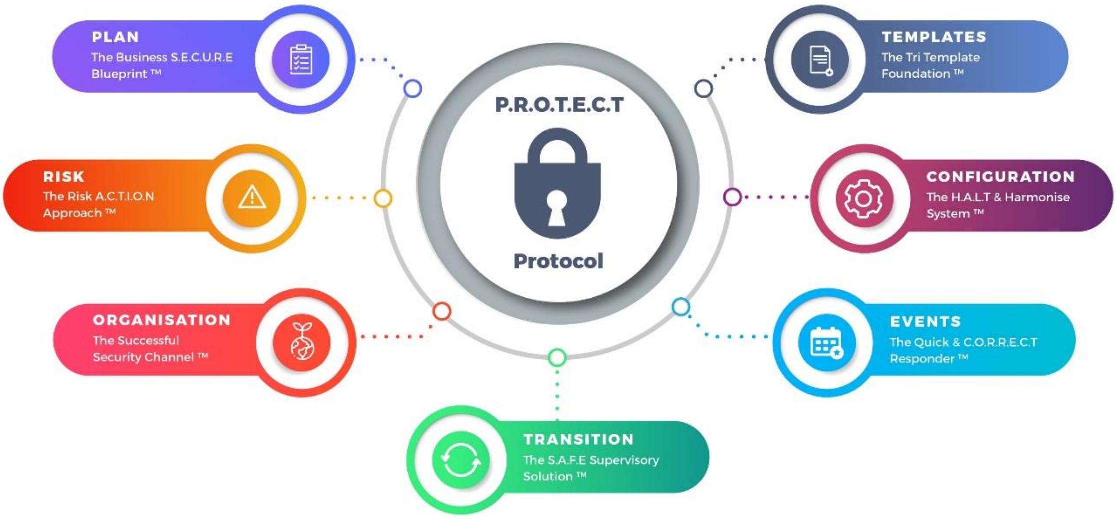
This solution tackles all the major sticking points that all businesses I come across commonly suffer from, for security and compliance. It:

- ✓ SAVES time training staff about the foundation they actually need to know/use in security without a 3-year University Degree or certification.
- ✓ SAVES the business from spending money on the wrong tools/tech for them.
- ✓ Shortens the time for a business to get securer, faster.

There are so many things we want to share with you from The PROTECT Protocol™, but we simply do not have time to do this in just one article. Therefore, the intent of this article is to help you get started, by doing an overview and giving you some top tips, to help point you in the right direction. You will then have a clearer view of security and what you wish to do for next steps.

Sounds good? Let's get started.

The 7 Stages: P.R.O.T.E.C.T


P.R.O.T.E.C.T
Protocol
PLAN
The Business S.E.C.U.R.E Blueprint ™
TEMPLATES
The Tri Template Foundation ™
RISK
The Risk A.C.T.I.O.N Approach ™
CONFIGURATION
The H.A.L.T & Harmonise System ™
ORGANISATION
The Successful Security Channel ™
EVENTS
The Quick & C.O.R.R.E.C.T Responder ™
TRANSITION
The S.A.F.E Supervisory Solution ™

There are seven keys areas that you need to master to improve your security fast. You do not need to do all these, but the more your do, not only will you be more secure, but these elements will also help you become a more mature company that is more resilient. One thing you need to understand it is an ongoing security journey, and this means continuous improvement.

PLAN

Out of all the elements, PLAN is the most important. You need to follow a plan, that is simple to understand, and be able to cover the important steps to manage security. You see many businesses are very reactive, whereby they have a problem, then put in place tools/technology to fix that and move on. That is not security. Security is ongoing, therefore it needs to be managed in the right way. This means you need to put processes in places to identify the right things to protect that is important for the business, ways to understand and measure how secure you actually are, ways to avoid just spending money on technology, and making sure those fixes are done correctly. Without that, business do not really understand how secure they are, and will be continually firefighting and being reactive, especially when there is a data breach.

RISK

Do not fall into the trap of isolating data security as an 'IT problem'. In any mature business, you will find management of risk is key. Data security/IT security is also a risk, therefore you need to put foundational elements to calculate risk. What many businesses do not have is a proper risk management process, to really understand what are the biggest risks to the business at that point in time, which leads to poorer decision and potentially ignoring important risks to data and security. You need to follow a proper risk management process, this helps your business focus and prioritise what it important for the business, what the business will tolerate and what the business will not tolerate. What you must also do is understand the 4 key elements how to handle a risk, which leads into what risk action approach you will take. These steps better your business in its decision making, justify its decision making, and undertake better choices and appropriate actions to manage that risk.

ORGANISATION

What this means is that your business needs to sort out how to organise itself to embed security. Without ways to embed security, you will be fighting against management to do the things you want to do, you will be fighting with more hands-on staff as they just don't understand security. What you need to do is to ensure you have ways to gain management support, which also means you will need clear lines of communication to management without having biased views, nor people reporting their own homework. You will also need ways to make staff understand security and know what to do to identify a potential problem and report an issue. Many businesses fail to do this, what this leads to is constantly having challenges to ask for budget or more staff; lack of time to do security; constantly being ignored by management; having problems when staff do something wrong, of which could have been prevented.

TRANSITION

Businesses implement change and this means this can result in things breaking, or worse, things introducing a security risk. New business processes, and new technology processes have the potential to lead to a data breach. There has been instances where businesses have made a transition or change – for example:

- ✖ a new online system that could expose your database of customer information.
- ✖ install a patch that breaks processes downstream.

I have come across the above and more. This has a big impact to customers, your services and later consequences for the business. When you get this right, you will have implemented processes to have a better idea of the change, the risks it could cause, have a plan B set and checks to make sure everything is working as expected. This minimise the chance of things breaking, and data security being affected.

EVENTS

What happens is that eventually your business will suffer an incident. It's inevitable. The quicker the business accepts this fact, the more you can do about it. You see many businesses simply have not thought enough about how to manage a security event, because they do not have these processes in place.

What you need to do is first put processes in place to understand what is a security incident or what is not. You do not need to consider every single security issue as an incident. If you do consider every security issue as an incident, you will spend too much time and not focus on the things that really matter. If it is a confirmed incident, then make sure you have the right teams in place to bring in at the relevant times (not just IT staff), then make sure you have good responses and recovery procedures for those critical systems. After this, you need to have follow processes to minimise the chance of this happening again. You see businesses who do not get this right, often do not solve the problem, which means they can get attacked and successfully breached again – we hear about this time and time again. But if you do put these processes in, your business will evolve over time and get more resilient – you will know what to do, know how to react quicker and minimise the risk of consequences.

CONFIGURATION

It goes without saying that you need to configure your systems securely. It is disappointing to see that too many businesses I come across don't do this right, or not covering the systems that should be configured. They may have a go, but often do not really know how to secure the systems because they only use their experience, their memory and little is documented and not repeatable. It is like asking one person to configure your phone securely, then asking someone else to configure it securely. What you will then realise is that it was not configured in the same way and therefore security features may not be implemented. Same when you talk about configuring other endpoints like laptops and network devices.

What you need to learn is where to find this information, what should be configured and also how to configure the right things to harmonise your systems. What I mean by harmonise is the systems are configured to work together, so it helps identify/highlight if you have a security issues, and if you do that you get the right information you need to support you in an incident. Key areas I find where business fail this are not properly configuring systems such as your websites, your anti-virus, and the ever so important database, which is very shocking - do not forget these.

TEMPLATES

In short, you need to understand the basic principles of security, which helps you realise why and how all these different elements come together. In any business, you need to set the tone from management down. Therefore, you need to have the right policies, which will drive security into your procedures. These fundamental templates are required to build that security foundation, you need to put these Lego bricks of security on top of. You will need to develop your own proper templated policies, and to save you time, when you join The PROTECT Protocol™, you will get these simple templates that you will adapt for your business to get you there super fast and you get these for free.

Next steps

So there you have it, those are the key areas that you need right now to supercharge your data security. Improve those areas with the top tips.

Of course, we would welcome you to be a client in the future and be a success story. So, if you are serious in improving your security fast with The PROTECT Protocol™, just arrange a discovery call with us. Email us at: info@minervasecure.co.uk