Security is not a tool and your tools are not security

Limitations of security tools

Taz Wake
Halkyn Consulting Ltd
Security & Risk Management Specialists

Security is not a tool and your tools are not security

Quite rightly, information security is a hot topic for most businesses. This is driven by a combination of regulatory and legal compliance pressures and the unavoidable fact that information (data) has become a valuable asset which needs to be properly protected and managed.

This is where good information security practices come in. With good security measures you can reduce the chances of a data loss event, regulatory fine or public embarrassment and loss of share price. Good security can also help you stand out from the competition in a crowded market and is often mandatory to win certain contracts (such as Government related work).

Good information security comprises a blend of policies, standards & procedures, properly followed by well trained and security aware employees, all of which is monitored and assured by technological implementations.

Unfortunately there is a growing trend across all sectors to sacrifice the foundation aspects and fall back on the strange idea that the latest Security Tool from [Insert Vendor Name Here] is the be-all and end-all of security.

This is a major failing and one which, if allowed to go unchecked, can significantly undermine your entire organisations approach to securing its data and information assets.

Saying this isn't the same as saying security tools are bad, just that all technological controls must be part of a bigger security picture and as an organisation you need to be painfully aware of the limitations they carry – making sure you bolster them with good people and process controls.

The problem is that once an enterprise has spent $1m on implementing security tooling across the estate, often there is little else left for the important bits. If your CISO (you do have one, don't you?) allows this to happen, you have pretty much put the cart before the horse and should think about making some major changes.

Things that should be considered include:

Security tools are mindless and can never replace a risk management approach to security. By their very nature, security tools fall into the doomed security approach of having a checklist of items and demanding that everything falls into the same sets of boxes. Tools can provide useful information for the risk management plan, but they can't replace it and if you start to become too reliant on the tool output, you will discover your security team have de-skilled themselves and simply rely on checklists to do their work. At this point, you have ceased to provide risk managed security for your enterprise.

Security tooling is only as good as the person who deploys it. Most tooling gets configured to your environment, leaving you reliant on the skill level, knowledge and experience of the person driving it. People make mistakes and people overlook things – if you become too reliant on the security tool output, small operator errors can magnify to create a critically distorted picture of your security environment.

Security tools can only test technical things. Despite what a lot of people think, IT Security and Information Security are about a lot more than bits and bytes being sent over the wire. It is about more than the routers, the servers, the switches and the hubs. All international standards (ISO 27001/27002, SOGP etc.) have a variety of control areas that can't be covered by security tools (such as Annex A.8 of ISO27001 looking at HR Security) and it is very likely that your security policies include requirements which are not suitable for automated testing.

Even the PCI-DSS standard, which is largely geared towards allowing for automated compliance scans, has controls which fare badly on this measure (requirements 7 and 9 are good examples of things which need a human to look at it and thing about it.).

Tooling checks things which can be automatically scanned – such as server build configurations – but that is pretty much it.

Using lots of security tools doesn't always improve the coverage. It is good practice to use at least two layers of firewall from different vendors and it is good practice to use a different Antivirus for your servers and desktops. Unfortunately this good practice advice is

frequently taken to the extreme with security tooling. We have worked with clients that have installed multiple Security Information and Event Monitoring (SIEM) tools, as well as Security Event Monitoring (SEM) and Enterprise Security Manager (ESM) tooling – all of which produces a monumental overlap in reporting. The principle of using two different vendors is sound normally, but in the monitoring world it leads to two problems (one big, one small):

- Multiple tool reporting distorts the perception and metrics leading to wildly inaccurate conclusions about the state of security on the enterprise. The tools are not necessarily providing correlation reporting, so you have to spend a lot of time making sure that each is scanning properly and independently as well as ensuring the reporting is on a like for like basis.
- Different vendor names don't always mean different vendors. Yes this is a small issue, but it means that if a certain vendor has a programming issue which leads to vulnerabilities, it is likely to exist on all products.

Again, the key here is the obvious yet overlooked principle of making sure you fully understand the limitations of your tools. Do not try to sell them as the silver bullet of security, instead be realistic and honest.

So, are security tools bad?

The answer is an emphatic **NO**. Security tooling has a very valuable place in every security risk management plan and every organisation, whatever the size, should ensure they at least consider implementing tools to support the security function.

This is the key point: **Security tools must support your security function**. If you are bringing in tooling to reduce costs, reduce headcount or shrink the security department, you are making a serious mistake which is likely to lead to major problems for your organisation in the future.

Before you reach for the catalogue and help make sure your preferred vendor can take their kids to Disney for Christmas, make sure you are doing it for the right reasons, in the right way.

Security tools must be built into an existing good approach to security and that means after you have worked out your organisations risk appetite, produced solid, workable security policies / plans / standards (etc.), and made sure you have the right people doing the right jobs.

If your approach to security is flawed, bolting on a security tool won't fix it. All you are doing is throwing away a lot of money.

Don't be that business.

About Halkyn Consulting

Halkyn Consulting Ltd is a specialist security consultancy based in North Wales, experienced in providing security advice to local, national and international clients including government agencies, multinational corporations, small businesses and homeowners.

For more advice on how to properly use passwords or any other questions you may have related to security and protecting your home, business or other assets, you can reach Halkyn Consulting at www.halkynconsulting.co.uk or info@halkynconsulting.co.uk.