Basic cybersecurity hygiene: 5 inalienable truths.

CRMG
CYBER RISK MANAGEMENT GROUP

At CRMG we don't have an aversion to the array of highly impressive products and services that compete for the modern CISO's budget. As an example, the role that artificial intelligence (AI) can play in speeding up an organisation's targeted response to a new breach is exciting. Where once a team of analysts might scramble to understand the implications of a piece of malware found on the corporate network – and err on the cautious side when deciding whether to advise pulling the plug on critical business systems - increasingly sophisticated tools can now instantly determine (and execute) exactly what containment measures are needed without bringing the organisation's operations to a screeching halt.

Irrespective of the pace of technical advances that increase our firepower in combatting the cyber threat, there remain a number of inalienable truths that mean we can't ignore the importance of 'basic cybersecurity hygiene'. Here are '5 truths' that explain the point.

Truth #1:

Don't forget it's still all about the information.
There's a reason why those of us who've been kicking about for a while in the cybersecurity industry used to call it 'information security'. 'Cybersecurity' is no more than 'information security' on the steroid we know as the Internet. Just because the Internet introduced new threats, attack surfaces, and accelerated the ability of nefarious entities (individual, corporate or nation state) to cause untold mayhem, the underlying principle hasn't changed. IT'S STILL ALL ABOUT THE INFORMATION.

Since the dawn of mankind information has accrued value for its owner. Information is a competitive advantage. Information is intelligence about our customers that enables us to sell services to them without incurring undue risk. Information is the blueprint for the self-driving car that can tell the difference between an elderly lady about to cross the road and a traffic bollard. Information is the finer detail of the due diligence activity on which our next investment round is predicated.

Information is a commodity no less valuable than hard currency, and in many cases it's way more valuable.

Truth #2:

Not all information is created equal.
Assuming you accept Truth #1, it follows that it's only worth getting out of bed to protect the information that you're really bothered about. If you have no means by which you can value the information on which your organisation thrives (assuming you don't have an infinite information protection budget), you might as well pack up and go home. The information you're really bothered about is entirely a subjective matter of course. That's why purchasing off the shelf cyber products and services – without understanding whether you're genuinely focusing on what matters – runs the risk of being the equivalent of buying up the entire stock of Fortnum's ground floor on 22 December just because the in-laws are popping round for a mince pie and a sherry on Christmas Eve.

Truth #3:

Sometimes what YOU think doesn't matter.
Sometimes, the decisions you make as to whether it's worth protecting (or not) the information your business holds might just not be up to you. Something as simple as building a database of phone numbers and e-mail addresses of those you

think might be interested in your services will, of course, incur the wrath of regulatory bodies if said database doesn't meet the requirements of data protection regulations. Depending on your native industry and target market, you may be subject to regulatory requirements that are completely beyond your control, irrespective of the information you hold or the value you attach to it. And more often than not, these regulations will require baseline information security measures to be in place. No ifs, no buts. That's the nature of compliance.

Truth #4:

Information has a nasty habit of seeping all over the place.
Think of information as water that trickles throughout the arterial canals and rivulets of your organisation. Well channelled and protected, it enables the business to thrive. Leave a sluice gate open inadvertently and – to mix metaphors – you're toast.

Pinning down exactly where information resides, and protecting it only in the locations in which you THINK it SHOULD reside, is a very tricky business.

Even more so when you take today's complex ecosystems of supplier relationships into account – introducing the possibility that your network of arterial canals and rivulets extends into places way beyond your control. If you fail to apply a baseline level of protection throughout the entirety of your organisation (and its sphere of influence), you'll run a significant risk that information seeps out via channels you just didn't envisage, and didn't protect. Moving on to another analogy, ghosts really DO exist in the information world.

Even if you think you've disposed of information at the end of its useful life, the chances are that traces of it will still exist in multiple locations throughout the organisation. How can you be completely sure that staff haven't created copies of information that you just don't know about, and that these copies still don't exist? Without consistent implementation of baseline information security practices throughout the entirety of your organisation, you'll likely be exposed.

Truth #5:

The Robots ain't taking over any time soon.
The cyber workforce is still some way off. While AI is showing massive potential in all sorts of contexts, the human being as the ultimate decision-maker in our businesses isn't going anywhere fast. For the most part this is reassuring, not least because most of us aren't likely to be put out to pasture just yet by a new workforce of indefatigable, infallible robo-colleagues. The implication? Fallibility. Glorious, old-fashioned, human nature. Business decision-making tempered by human conscience. All good, until someone makes a glorious old-fashioned mistake, at which point you might wish that a robot had been in charge. Did that procurement manager really mean to share a dump of the entire customer database with that unvetted supplier? Ouch.

The point here is that, along with information, PEOPLE still represent most organisations' greatest asset. The problem is that, on the flip side, people also represent most organisations' greatest weakness.

Given that we're not yet able to implant chips behind the ears of employees to regulate reckless decision-making, we come back to the importance of basic security awareness. The articulation of meaningful, responsibility-riddled messages that resonate with staff, resulting in people refraining from doing bad things. It's not rocket science, but it's not easy either.

As your business matures you will inevitably turn to technologies to assist you in keeping your information safe and away from prying eyes.

Data Loss Prevention (DLP) technology is a great example. Well implemented, DLP can prove a great asset in preventing important information from filtering outside the organisation without you knowing about it. BUT – unless such solutions are supported by a consistent foundation of straightforward, well understood, information security good practices – you're taking a huge risk.

This is why no CISO can afford to ignore basic cybersecurity hygiene. And if this argument doesn't persuade you, your regulators most probably will.

So, what specifically are we referring to when talking about basic cybersecurity hygiene? Here are just some baseline good practices. Just to add context I've related them back to the 5 truths:

#1 If you haven't done so recently, embark on an information discovery exercise. At its simplest, this might start with a simple map of your key business processes and information systems that support them. Don't forget to explore instances where information is shared between systems/functions and – just as importantly – to identify where information is shared outside the organisation. This activity doesn't have to be sophisticated (at least at first).

You just need to come away from it with a high level of confidence that you understand what information lives in your organisation, where it lives, and who interacts with it. As a tip, it can be really useful to run this exercise as a workshop that includes both technical and business people (or a series of workshops if your organisation is large or dispersed).

You'll be surprised at what can get unearthed... did you have any inkling that Mervyn in Accounts routinely does a monthly .csv export of all employee data and shares it with your outsourced benefits management provider via a cloud drive that goes nowhere near your protected corporate network?

#2 Once you have your basic map of what information lives where in your organisation, it's a good idea to have a crack at valuing it in some way. This might be as simple as identifying what information your business can't function without. By implication everything else will be slightly less important.

Once you understand the relative value of different information types or systems, you'll then know where information protection efforts should be focused – because the realities of business economics tell us that in most cases it just isn't possible to apply the same level of protection to absolutely everything throughout the organisation.

By the way, possibly without knowing it, by this stage you'll have worked through the first steps of a basic information risk assessment (but we'll save that for another day).

#3 This is all about regulatory compliance. All sorts of businesses face all sorts of compliance requirements. The point here is that you must take the time to understand exactly which laws and regulations you're required to comply with by virtue of your business activities and the information you hold. While highly regulated sectors (such as Finance, Insurance and Healthcare) have been used to managing compliance requirements for many years, there's a whole new generation of businesses that have only really been forced to start taking notice of compliance because of GDPR.

Once you know what regulations you're required to comply with, you'll then need to understand EXACTLY what measures you're required to have in place to comply with them. If you don't spend money on consultancy anywhere else, this is one area where it's probably a good idea to call in an expert to help you.

#4 Notwithstanding any beefed-up protection you apply to your most important information, you still need to implement a baseline set of security measures throughout the entirety of the organisation. This includes things such as:

- Developing a straightforward information security policy that is accessible by every employee and which clearly states exactly what is required by staff to protect the information handled throughout the business
- Making sure that all employees are aware of their information security responsibilities (more on that below)
- Liaising with key suppliers / partners to ensure they are operating to a minimum, defined, information security standard
- Keeping all systems patched and up-to-date, and checking this routinely
- Ensuring all systems and end devices are installed with up-to-date anti-malware software
- Having specialist support available on speed dial if something does happen that you can't manage yourself!
- Only providing staff with access to systems if they really need it (when you do, make sure that access rights aren't excessive - and don't forget to revoke them once they've moved to a different function or left!)
- Encrypting particularly sensitive information (remember that even if personal data isn't critical to your business' success, you're still required by law to apply strict controls when storing or handling it)
- Maintaining backups – and testing them periodically
- Implementing business continuity and disaster recovery procedures (even if they're basic) that support 'business as usual' as far as possible in the event of an incident
- Working with a credible third party to undertake a periodic penetration test of your systems – and making sure any recommendations are applied

#5 Good information security awareness is critical to any business these days, and you just can't afford to skimp on it. So, think about the basic information security good practices you want ALL staff to be aware of, and come up with an engaging way of ramming the message home. Be creative. Incentivise. Draw a picture. Make a video. There's a reason why those opting to attend a driver awareness course instead of getting slapped with extra points on their license get shown the horrific aftermath of traffic accidents. Whatever approach you choose (and remember it doesn't need to cost a fortune and it doesn't have to be cast in stone... you can try different methods over time), just make sure you do it. And do it again.

Also have a think about whether there are specific roles in the business that require an additional level of training – particularly those handling sensitive information. Lastly, remember that people – just like information – have a habit of moving about. Don't forget that when new people join, staff move to new roles in the business, or when they leave, you'll need to have a clear process to make sure they're getting the right security awareness training at the right time.

None of what I've outlined above should be considered to be advanced if your organisation conducts its business using the Internet (and whose business doesn't?). There's plenty more you'll need to do as your business matures. We haven't even mentioned cybersecurity strategy, threat profiling, and so on.

If you choose to skip any of the basic hygiene measures I've outlined relative to Truths #3, #4 and #5, have a long hard think, because you might not have a business left to mature if you ignore them. Choose to ignore the guidance related to Truths #1 and #2, and you'll have to protect everything to the highest level just to be sure – which in an extreme case might just amount to the same thing.

Simon Rycroft is a Co-founder and Director of CRMG
simon.rycroft@crmg-consult.com | www.crmg-consult.com