Getting to grips with cyber security

The common and somewhat fatalistic rhetoric is that it's not a case of if a business will suffer a cyber attack, but when. If we believe this, we are all doomed. But there are fairly straightforward things your business can do to help avoid being a victim, says **Gary Fairley**

Every incident has its JFK moment. Where were you when everything went horribly wrong? My particular 'favourite' was walking into one of our offices to deliver a presentation about the perils of phishing when my phone rang. At the other end of the line was my harassed security administrator, telling me: "We think we've got a server with ransomware on it. What do we do?" Oh, how we laughed about that one. Much, much later.

Fast forward six months or so, and I had just walked in the door at home one Friday afternoon when my wife pointed at the television. News of a cyber attack crippling National Health Service (NHS) systems had broken. While I didn't work for the NHS, my own organisation worked very closely with it, sharing buildings, data, systems and staff.

Through the gaps between my fingers, I could see that my in box was filling up nicely, not with emails telling me of a gathering storm at the periphery of my network, but with dozens of cyber security vendors selflessly marketing their wares in light of the "recent NHS cyber attack." At this point the attack was, more accurately, still actually happening. There may be honour among thieves, but apparently less so among IT salespeople and account managers.

Trawling through the exclusive white papers, Ten Easy Steps to Salvation and tips on how to combat the insider threat, I found what I had been looking for: we were okay, or at least we were reasonably certain that we were, for the time being anyway.

As news of the impact of what we now know as the WannaCry attack filtered in that evening, I started to think. Just how many people clicked on the link or the email attachment? How many emails were sent? How did it spread so quickly? Just how flat are their networks?

But there wasn't a link. There hadn't been an email. Nowhere was there a harassed junior doctor who had unwittingly opened a spurious invoice or clicked to see the progress of some forgotten delivery. And it wasn't just the NHS or even just the UK. FedEx, Deutsche Bahn, Telefonica, Renault and Nissan were names being added to the list of those affected.

That evening, I watched UK Government Home Secretary Amber Rudd telling reporters that everything was under control and that the NHS practised for this sort of thing: "All the time". Did I detect a slight squirm from the man stood next to her – Chief Executive of the UK's National Cyber Security Centre, Ciaran Martin?

When you see hospitals and doctors' surgeries becoming victims of cyber attacks, you start to contemplate dark realities. My principles have a number of sacred cows, the NHS probably being the biggest one. Meddle with that, my friend, and you risk swift and uncompromising retribution; perhaps a strongly worded email or 140 barbed characters on Twitter, and don't say I didn't warn you.

> Cyber security is still viewed in many circles as an IT problem, to be fixed by IT people with IT equipment. This has to change

Was this an attack on the UK's critical national infrastructure? If so, then my breezy messages about 'People, policy, passwords and patching' were suddenly looking positively precarious, poor and past-it.

The scale of the WannaCry attack sets it apart from other incidents. An estimated quarter of a million computers are thought to have been affected in over 150 countries. WannaCry wasn't exactly a couple of teenage 'script kiddies' running SQL scripts against a website.

But in many ways this was a fairly typical cyber attack. A known vulnerability, for which a patch was available, was exploited and ransomware was able to proliferate a number of systems.

It would have been easy to sneer as news emerged of obsolete, unpatched and unsupported systems. Windows XP? How quaint! But XP wasn't the issue and we would later learn that almost all of the infected computers were running Windows 7, a fact that I am certain will have focussed many minds.

What May's global cyber attack has shown us, apart from the ability of cyber criminals to strike on a worldwide scale, is that cyber attack is preventable, but that organisations are failing to get the basics right. Forget next-generation firewalls and industry-leading security incident event management (SIEM) capabilities, organisations are running out-of-date and unsupported software. They're trusting outdated networks, they're failing to refresh technology, they're failing to patch and they're doing so by choice. Or if not by choice, then out of ignorance.

Microsoft announced that the latest 'Patch Tuesday' release includes security patches for Windows XP, for which support ended no less than three years ago. Microsoft should be applauded for its sense of global social responsibility and I genuinely mean that. Any company may have legitimately questioned why it should restart supporting a product that most people abandoned years ago when better, safer, alternatives already exist. At what point does the responsibility for the security and resilience of an organisation's information and systems rest with the organisation itself?

Many observers have called WannaCry a wake-up call, but I wonder how many wake-up calls both public services and private business need. Cybersecurity is still viewed in many circles as an IT problem, to be fixed by IT people with IT equipment. This has to change. Cyber is a corporate risk that should be owned at the highest level and this is a message that seems not to be getting through to some.

I appreciate that cyber resilience isn't easy. It cannot be achieved overnight and needs investment of time and resources, constant monitoring and regular review – in many ways it's Deming's classic 'Plan, do, check, act' cycle.

- **Plan**: The first step is arguably the most difficult and lies in understanding the risks to information and systems. What are the organisation's information assets? What are the critical systems and what would the business impact be if they were compromised in any way? These are key questions in helping make cyber a priority for any business.

It is from here that you can begin to develop incident management and disaster recovery plans and the procedures to respond to any incident.

- **Do**: Prevention is always better than cure so be sure to implement your cyber security policies, controls, processes and procedures. So, just as you would any building, protect your network from unauthorised access. Establish perimeter defences, using firewalls and appropriate anti-virus controls. Filter email content to guard against viruses, malware, spam and other nasties. Monitor web traffic for signs of unusual activity that may indicate the presence of malware inside your network. Establish appropriate anti-virus controls, from the outside of your network in. Cover gateways, servers, switches, routers, PCs, laptops, mobile devices, the lot. Also segregate your network – do you really need a connection between the finance system and the corporate website? Or, for those of you familiar with the Target breach in 2013, why can someone access your payment systems from the air conditioning system? Protect sensitive systems with additional firewalls or other controls.

Configure your systems securely. As we already know, WannaCry exploited a known vulnerability and an alarming percentage (ie most) of breaches are as a result of misconfigured and unpatched devices.

Consider deploying a standard build for your devices, with only relevant or essential features enabled. Does a feature benefit your business or does it just introduce risk? Does everyone need write access to USB drives? Manage the exceptions by group policies. Also change any vendor default passwords on devices and consider restricting internet access.

Use the principle of least privilege, give people the lowest level of user rights to do their job. Does your CEO really need enterprise admin rights, or your CFO access to the back end of the finance system? Also limit the number of privileged (or admin) accounts and establish procedures for the creation of these. Monitor their use and remove privileges when no longer required.

People are actually your strongest link. Let staff know what's expected of them, train them, help them understand what to look for, how to spot phishing emails and the like, and let them help you keep things secure. Make sure your policies and controls are secure enough to do the job without being too onerous. Make things too difficult and people will actively seek ways of getting around them, not out of malice, but out of a desire to simply get on with their jobs.

Unusual activity

Back your data up. What would happen if you were hit with a ransomware attack? Restoring from back-up is often the only way of recovering from a ransomware attack. But make sure it's accessible quickly, whether from the cloud, in-house or off-site storage.

- **Check:** Monitor your systems and your network. What's actually happening inside your organisation? Where's data going or coming from? Analyse system logs for unusual and/or unauthorised activity.

Test your network for vulnerabilities, particularly new systems and those that manage sensitive information. Test incident management and disaster recovery plans and make sure the key players are involved. Include your back-ups. It's no good backing up data to discover that it has been corrupted or lost when disaster strikes.

- **Act**: Take corrective and preventative action. Fix what's broken, monitor and review what isn't. Look beyond your network: how secure is your supply chain? How do you know?

And repeat as necessary.

This is not a manifesto for 100 per cent assurance but, by taking reasonably basic steps, a business can protect itself against a majority of threats that lurk in what is now known as the Internet of Things.

You could almost call it 'People, policy, passwords and patching'. Now, didn't I just type that somewhere…? CRJ

At a glance

At what point does the responsibility for the security and resilience of an organisation's information and systems rest with the organisation itself?

People are actually your strongest link, if they are trained properly

Make things too difficult and people will actively seek ways of getting around them, so as to get on with their jobs

Samuraitop | 123rf

Author

GARY FAIRLEY *used to be an IT Security Manager in the Scottish public sector. Having apparently sold his soul, he is now plying his trade in the private sector*